NORTEL NETWORKS

BASE PROTOCOL SPECIFICATIONS

Confidential

IP Mobility Group

Nortel Networks
2221 Lakeside Boulevard
Richardson, Texas 75082, USA

Publication History

Revision	Date	Reason	Author(s)
Original Draft	July 20, 2000	Initial draft.	Linda Sides

DRAFT - For Review Only

Nortel Confidential

EXHIBIT 2 PAGE 11 OF 130

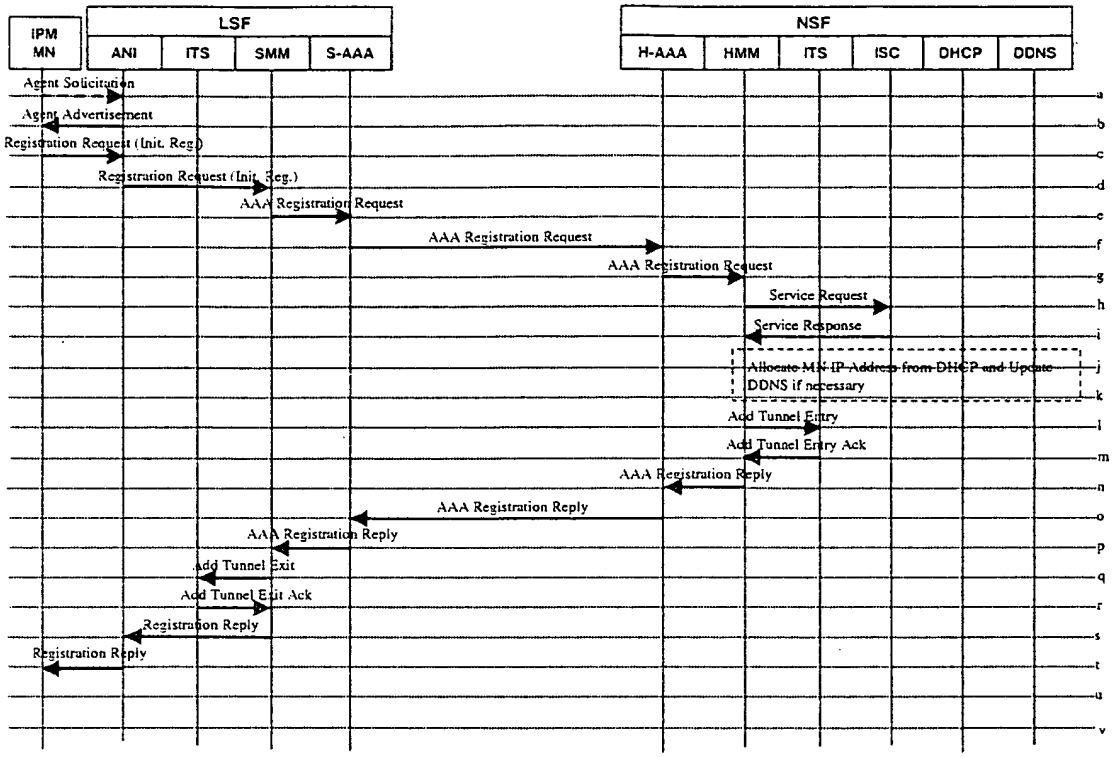
1. INTRODUCTION

This Page Blank (uspto)

DRAFT - Nortel Networks Confidential

2. IPM MESSAGE FLOWS

2.1 IPM MN REGISTERS FROM THE IPM LSF



IPM MN registers from IPM LSF

2.1.1 Agent Discovery Process

Agent Discovery is the method by which a mobile node determines whether it is currently connected to its home network or to a foreign network, and by which a mobile node can detect when it has moved from one network to another. Home agents and foreign agents may advertise their availability on each link for which they provide service. A newly arrived mobile node can send a solicitation on the link to learn if any prospective agents are present. The Agent Discovery Process is primarily handled through Agent Solicitation and Agent Advertisement.

2.1.1.1 Agent Solicitation and Message Format

Agent Solicitation is the broadcast/multicast message sent by the IPM MN to detect a Service Provider in the event that the IPM MN has not received an Advertising Agent message.

The **message format** exchanged between the IPM MN and the ANI is as follows:

Type	Code	Checksum
Reserved		

- **Source Address** – An Mobile IP address belonging to the interface from which this message is sent, or 0. This is part of the standard heading.
- **Destination Address** – The configured Solicitation Address. This is part of the standard heading.
- **Type** – 10
- **Code** – 0
- **Checksum** – The 16-bit one's complement of the one's complement sum of the ICMP message, starting with the ICMP Type. For computing the checksum, the Checksum field is set to 0.
- **Reserved** – Sent as 0; ignored on reception.

There are no Extensions for Agent Solicitation.

2.1.1.2 Agent Advertisement and Message Format

Agent Advertisement are messages sent periodically, either as a broadcast or multicast for the visiting IPM MN to recognize the availability of service and to keep track of their point of attachment.

The **message format** exchanged between the ANI and the IPM MN is as follows:

Type	Code	Checksum
Num Addrs	Addr Entry Size	Lifetime
Router Address [1]		
Preference Level [1]		
Router Address [2]		
Preference Level [2]		

- **Source Address** – An IP address belonging to the interface from which this message is sent. This is part of the of the standard heading.
- **Destination Address** – The configured Advertisement Address or the IP address of a neighboring host. This is part of the of the standard heading.
- **Type** – 9
- **Code** – 0
- **Checksum** – The 16-bit one's complement of the one's complement sum of the ICMP message, starting with the ICMP Type. For computing the checksum, the checksum field is set to 0.
- **Num Addrs** – The number of router addresses advertised in this message.
- **Addr Entry Size** – The number of 32-bit words of information per each router address (2, in the version of the protocol described here).

- **Lifetime** – The maximum number of seconds that the router addresses may be considered valid.
- **Router Address [i], i = 1..Num Addrs** – The sending router's IP address(es) on the interface from which this message is sent.
- **Preference Level [i], i = 1..Num Addrs** – The preferability of each router address [i] as a default router address, relative to other router addresses on the same subnet. A signed, two-complement value; higher values mean more preferable.

The Extensions that can be used in Agent Advertisement Message are,

- **Mobility Agent Advertisement Extension**
- **ANI-NAI Extension**

and can be explained further in the Extension Section 4.

2.1.2 Registration Process

The purpose of registration is for the IPM MN to inform the HMM of the NSF (Network Serving Function) of its current location to which data packets can be forwarded to the IPM MN. The Registration process also includes the authenticating and authorizing of the IPM MN to have access to the visited network or LSF (Local Serving Function).

2.1.2.1 Registration Request and Message Format

The Registration Request Message is sent by the IPM MN to the SMM to register for the service.

The **message format** exchanged between the IPM MN and the SMM is as follows:

Type (8)	Flags (8)	Lifetime (16)
Home Address (32)		
Home Agent (32)		
Care-of-Address (32)		
Identification (64)		

- **Source Address** – An IP address of the MN. This is part of the standard heading.
- **Destination Address** – The COA within the ANI component. This is part of the standard heading.
- **Type** – The type of the message is "0", which is the Registration Request Message.
- **Flags** – The flags filed are the same as RFC2002.

- **Lifetime** – The lifetime requested by MN from the HMM or Home.
- **Home Address** – The IP address of the Mobile Node.
- **Home Agent** – The Home Agent's address of the Mobile Node.
- **Care-of-Address** – The Care-of-Address of the Mobile Node.
- **Identification** – The identification, to provide replay protection.

The Extensions used in the Registration Request are,

- **User-NAI Extension**
- **L2-Address Extension (Optional)**
- **MN-Home Authentication Extension**
- **Registration-Type Extension**
- **Previous-SMM-NAI Extension (Optional)**
- **ANI-NAI Extension (Optional)**
- **MN-SMM Authentication Extension (Optional)**
- **ANI-SMM Authentication Extension (Optional)**
- **ANI-HMM Authentication (Optional)**

and can be explained further in the Extension Section 4.

2.1.2.2 AAA-Registration Request and Message Format

The AAA-Registration-Request Message is used to carry out various kinds of registrations; these registrations are encapsulated in the IPM-Registration-Type AVP. This message is used by SMM to authenticate and authorize the user.

The message format exchanged between the SMM and the HMM is as follows:

AAA-Registration-Request	<DIAMETER Header>
	<Command-Code AVP = 335>
	<User-Name AVP>
	<Host-Name AVP>
	<IPM-Registration-Type AVP>
	<IPM-Registration-Request AVP>
	<IPM-Care-of-Address AVP>
	<IPM-Routing-Area-NAI AVP>

The AAA-Registration-Request Message is of the format of DIAMETER. The SMM sends the message to HMM with at least these mandatory fields. The IPM-Registration-Request AVP is the AVP which carries the message received from the MN, which is encapsulated in the AVP format for the Home domain to authenticate the user. The HMM processes this message based on the Registration-Type AVP, which carries the type of registration requested.

The AVPs that can optionally be used in the Registration Request Message are,

- **Destination-NAI AVP**
- **IPM-Client-Address AVP**
- **Home-Agent-Address AVP**
- **IPM-SMM-NAI AVP**
- **IPM-Terminal-Type AVP**
- **IPM-Profile-Type AVP**
- **Proxy-State AVP**
- **Timestamp AVP**
- **Nonce AVP/**
- **Integrity-Check-Value AVP**

and can be explained further in the AVP Section 5.

2.1.2.3 Service Request and Message Format

The Service Request Message is sent from the HMM to the ISC (IPM Security Center) to authenticate a user or message, generate, renew, or delete session secret keys. It also can be sent from the PPS Manager to the ISC to generate or construct the IPMC.

The **message format** exchanged between the HMM and the ISC is as follows:

Type	Sub-Type	Payload Length
Identification		
User NAI		

- **Type** – USER_SERVICE_REQUEST_MSG.
- **Sub-Type** – 0.
- **Payload Length** – Length of the message payload including all the extensions.
- **Identification** – A 64-bit number used for matching User Service Request Messages with User Service Reply messages, and for protecting against replay attacks of User Service Request messages.
- **User NAI** – In phase I, this Extension has the user NAI and in the future will have an index which will be used to index the user data in the UDS.

The Extensions used in the Service Request Message are,

- **User Authentication Information Extension**
- **Control Message Authentication Extension**
- **Session Key Allocation Extension 0..N**
- **Session Key Lifetime Renewal Extension 0..N**

- **Session Key Delete Extension 0..N**

and can be explained further in the Extension Section 4.

2.1.2.4 Service Response and Message Format

The Service Response Message is sent from the ISC (IPM Security Center) to the HMM in response to a Service Request Message.

The **message format** exchanged between the ISC and the HMM is as follows:

Type	Sub-Type	Payload Length
Code		
Identification		
User NAI		

- **Type** – USER_SERVICE_REPLY_MSG.
- **Sub-Type** – 0.
- **Payload Length** – Length of the message payload including all the extensions.
- **Code** – The following are the hex values of the defined codes:
  - 00000001 User Authenticated successfully.
  - 00000002 All required keys have been allocated.
  - 00000003 Some keys have been allocated.
  - 00000004 User Authentication failed.
  - 00000005 Key Lifetime Renewal is completely honoured.
  - 00000006 Key Lifetime Renewal is partially honoured.
  - 00000007 User Account is created successfully.
  - 00000008 User is deleted successfully.
- **Identification** – A 64-bit number used for matching User Service Request Messages with User Service Reply Messages, and for protecting against replay attacks of User Service Request Messages.
- **User NAI** – In phase I, this Extension has the user NAI and in the future will have an index which will be used to index the user data in the UDS.

The Extensions used in the Service Response Message are,

- **Control Message Authentication Extension**
- **Session Key Allocation Extension 0..N**
- **Session Key Lifetime Renewal Extension 0..N**
- **Session Key Delete Extension 0..N**

and can be explained further in the Extension Section 4.

2.1.2.5 Add Tunnel Entry and Message Format

The Add Tunnel Entry Message is sent by the HMM to instruct the ITS to set up a tunnel entry point.

The **message format** exchanged between the HMM and the ITS is as follows:

Code (16)	Message Length (16)
Identification (64)	
Extensions...	

- **Code** – 1, For Add Tunnel Entry.
- **Message Length** – Length of the message including the header fields.
- **Identification** – Is used in matching requests and acknowledgements. The sender must ensure the identifier in a message is locally unique at any given time.

The Extensions used in the Add Tunnel Entry Message are,

- **Host NAI Extension**
- **Flag Extension**
- **Lifetime Extension**
- **Mobile Node IP Address Extension**
- **User NAI Extension (Optional)**
- **Tunnel Entry IP Address Extension**

and can be explained further in the Extension Section 4.

2.1.2.6 Add Tunnel Entry Acknowledgement and Message Format

The Add Tunnel Entry Acknowledgement Message is sent by the ITS to acknowledge the "Add Tunnel Entry" Message.

The **message format** exchanged between the ITS and the HMM is as follows:

Code (16)	Message Length (16)
Identification (64)	
Extensions...	

- **Code** – 2, For Add Tunnel Entry Acknowledgement.

- **Message Length** – Length of the message including the header fields.
- **Identification** – Is used in matching requests and acknowledgements. The sender must ensure the identifier in a message is locally unique at any given time.

The Extensions used in the Add Tunnel Entry Message are,

- **Host NAI Extension**
- **Result Code Extension**
- **Mobile Node IP Address Extension (Optional)**
- **User NAI Extension (Optional)**

and can be explained further in the Extension Section 4.

2.1.2.7 AAA-Registration Reply and Message Format

The AAA Registration Reply Message is the response message sent by the HMM to the SMM to indicate the result of the AAA-Registration Request Message.

The **message format** exchanged between the HMM and the SMM is as follows:

AAA-Registration-Response	<DIAMETER Header>
	<Command-Code AVP = 336>
	<Destination-NAI AVP>
	<Host-Name AVP>
	<User-Name AVP>
	<IPM-Registration-Response-Code AVP>
	<IPM-Client-Address AVP>
	<IPM-Registration-Reply AVP>

The AAA-Registration Reply Message is of the format of DIAMETER. The HMM sends a message to the SMM with at least the mandatory fields in response to AAA-Registration Request Message. The IPM-Registration Response Code AVP indicates the success or failure of the request. The IPM Registration Reply Message AVP contains the reply message built by HMM with authentication. The SMM has to use this AVP to send a reply to ANI/MN.

The AVPs that can optionally be used in the Registration Reply Message are,

- **IPM-Profile AVP**
- **IPM-SMM-MN-Key AVP**
- **IPM-HMM-NAI AVP**
- **Proxy-State AVP**
- **Time AVP**
- **Nonce AVP**

- **Integrity-Check-Value AVP**

and can be explained further in the AVPs Section 5.

2.1.2.8 Add Tunnel Exit and Message Format

The Add Tunnel Exit Message is sent by the SMM to instruct the ITS to set up a tunnel exit point.

The **message format** exchanged between the SMM and the ITS is as follows:

Code (16)	Message Length (16)
Identification (64)	
Extensions...	

- **Code** – 3, For Add Tunnel Exit.
- **Message Length** – Length of the message including the header fields.
- **Identification** – Is used in matching requests and acknowledgements. The sender must ensure the identifier in a message is locally unique at any given time.

The Extensions used in the Add Tunnel Exit Message are,

- **Host NAI Extension**
- **Lifetime Extension**
- **Mobile Node IP Address Extension**
- **User NAI Extension (Optional)**
- **Tunnel Exit IP Address Extension**

and can be explained further in the Extension Section 4.

2.1.2.9 Add Tunnel Exit Acknowledgement and Message Format

The Tunnel Exit Acknowledgement Message is sent by the ITS to acknowledge the "Add Tunnel Exit" Message.

The **message format** exchanged between the ITS and the SMM is as follows:

Code (16)	Message Length (16)
Identification (64)	

- **Code** – 4, For Add Tunnel Exit Acknowledgement Message.
- **Message Length** – Length of the message including the header fields.
- **Identification** – Is used in matching requests and acknowledgements. The sender must ensure the identifier in a message is locally unique at any given time.

The Extensions used in the Add Tunnel Exit Acknowledgement Message are,

- **Host NAI Extension**
- **Result Code Extension**
- **Mobile Node IP Address Extension (Optional)**
- **User NAI Extension (Optional)**
- **Tunnel Forwarding IP Address Extension**

and can be explained further in the Extension Section 4.

2.1.2.10 Registration Reply and Message Format

The Registration Reply Message is sent by the SMM to the IPM MN to indicate the result of the Registration Request Message sent.

The **message format** exchanged between the SMM and the IPM MN is as follows:

Type (8)	Code (8)	Lifetime
Home Address (32)		
Home Agent (32)		
Identification (64)		

- **Type** – The type of the message is 3, which is the Registration Request Message.
- **Code** – All the existing MIP Response codes, this field is being extended to include IPM specific items.
- **Lifetime** – The Home lifetime for the registration.
- **Home Address** – The IP address of the Mobile Node.
- **Home Agent** – The Home Agent's address of the Mobile Node.
- **Identification** – The identification, to provide replay protection.

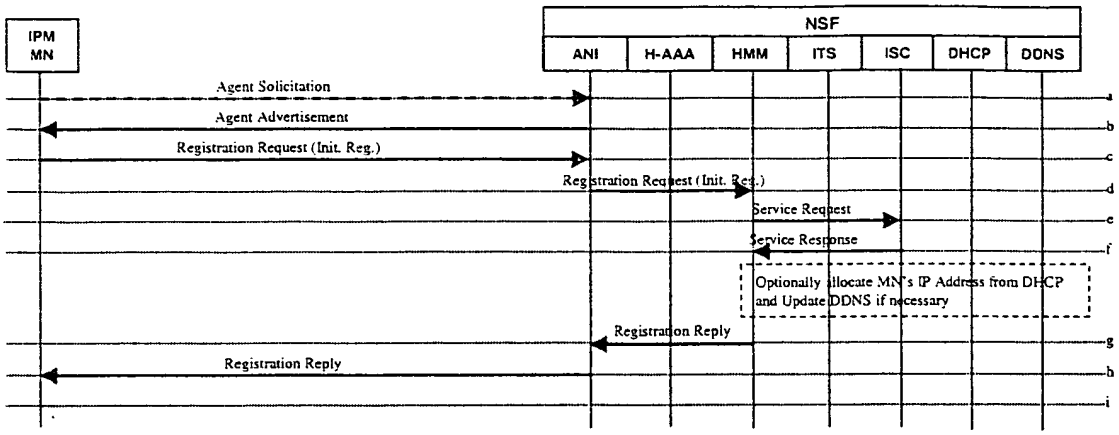
The Extensions used in the Registration Reply Message are,

- **User-NAI Extension**
- **SMM-Key Extension (Optional)**

- **MN-Home Authentication Extension**
- **Local Registration Lifetime Extension (Optional)**
- **SMM-NAI Extension (Optional)**
- **MN-SMM Authentication Extension (Optional)**
- **ANI-SMM Authentication Extension (Optional)**

and can be explained further in the Extension Section 4.

2.2 IPM MN REGISTERS FROM IPM NSF



IPM MN registers from IPM NSF

2.2.1 Agent Discovery Process

See Section 2.1.1

2.2.1.1 Agent Solicitation and Message Format

See Section 2.1.1.1

2.2.1.2 Agent Advertisement and Message Format

See Section 2.1.1.2

2.2.2 Registration Process

See Section 2.1.2

2.2.2.1 Registration Request and Message Format

The Registration Request Message is sent by the IPM MN to the HMM to register for the service.

See Section 2.1.2.1 for the message format exchanged between the IPM MN and the HMM.

2.2.2.2 Service Request and Message Format

See Section 2.1.2.3

2.2.2.3 Service Response and Message Format

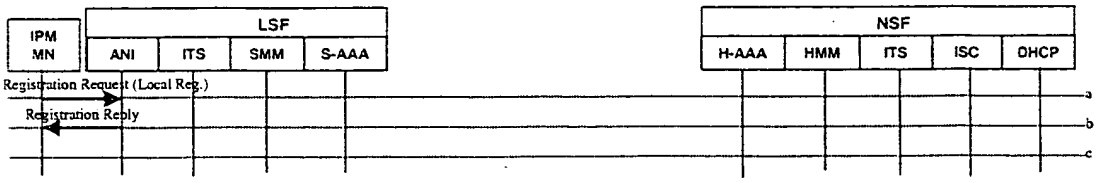
See Section 2.1.2.4

2.2.2.4 Registration Reply and Message Format

The Registration Reply Message is sent by the HMM to the IPM MN to indicate the result of the Registration Request Message sent.

See Section 2.1.2.10 for the message format exchanged between the HMM and the IPM MN.

2.3 IPM MN DISCONNECT DETECTION



IPM MN Disconnect Detection

2.3.1 Registration Process

See Section 2.1.2

2.3.1.1 Registration Request and Message Format

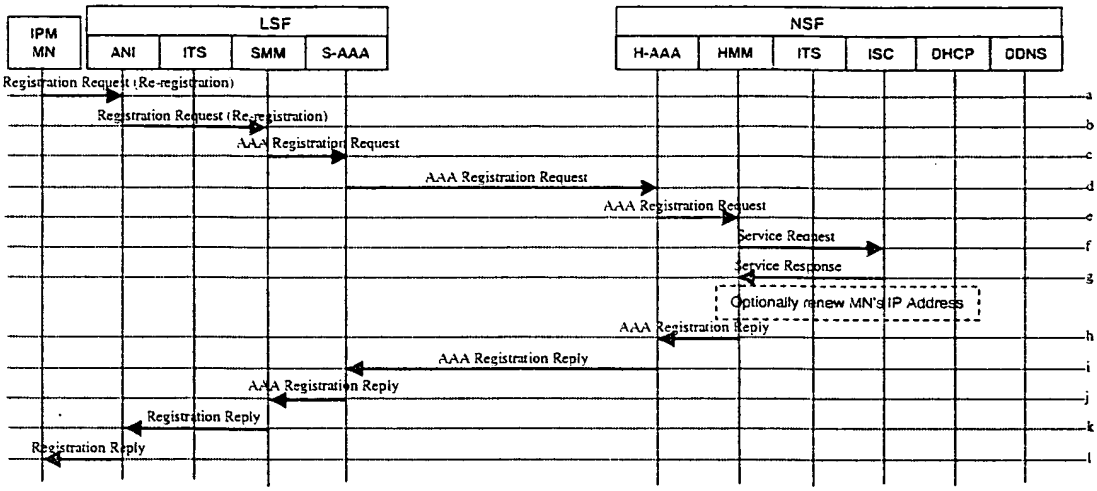
The Registration Request Message is sent by the IPM MN to the ANI when it detects a disconnect.

2.3.1.2 Registration Reply and Message Format

The Registration Reply Message is sent by the ANI to the IPM MN to indicate the result of the Registration Request Message sent.

See Section 2.1.2.10

2.4 IPM MN RE-REGISTERS FROM IPM LSF



IPM MN re-registers from IPM LSF

2.4.1 Registration Process

See Section 2.1.2

2.4.1.1 Registration Request and Message Format

See Section 2.1.2.1

2.4.1.2 AAA-Registration Request and Message Format

See Section 2.1.2.2

2.4.1.3 Service Request and Message Format

See Section 2.1.2.3

2.4.1.4 Service Response and Message Format

See Section 2.1.2.4

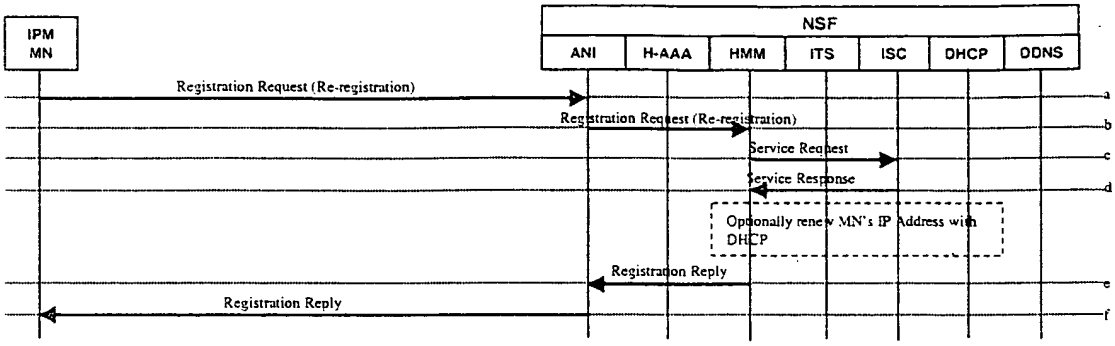
2.4.1.5 AAA-Registration Reply and Message Format

See Section 2.1.2.7

2.4.1.6 Registration Reply and Message Format

See Section 2.1.2.10

2.5 IPM MN RE-REGISTERS FROM IPM NSF



IPM MN re-registers from IPM NSF

2.5.1 Registration Process

See Section 2.1.2

2.5.1.1 Registration Request and Message Format

The Registration Request Message is sent from the IPM MN to the HMM to register for the service.

See Section 2.1.2.1 for the message format exchanged between the IPM MN and the HMM.

2.5.1.2 Service Request and Message Format

See Section 2.1.2.3

2.5.1.3 Service Response and Message Format

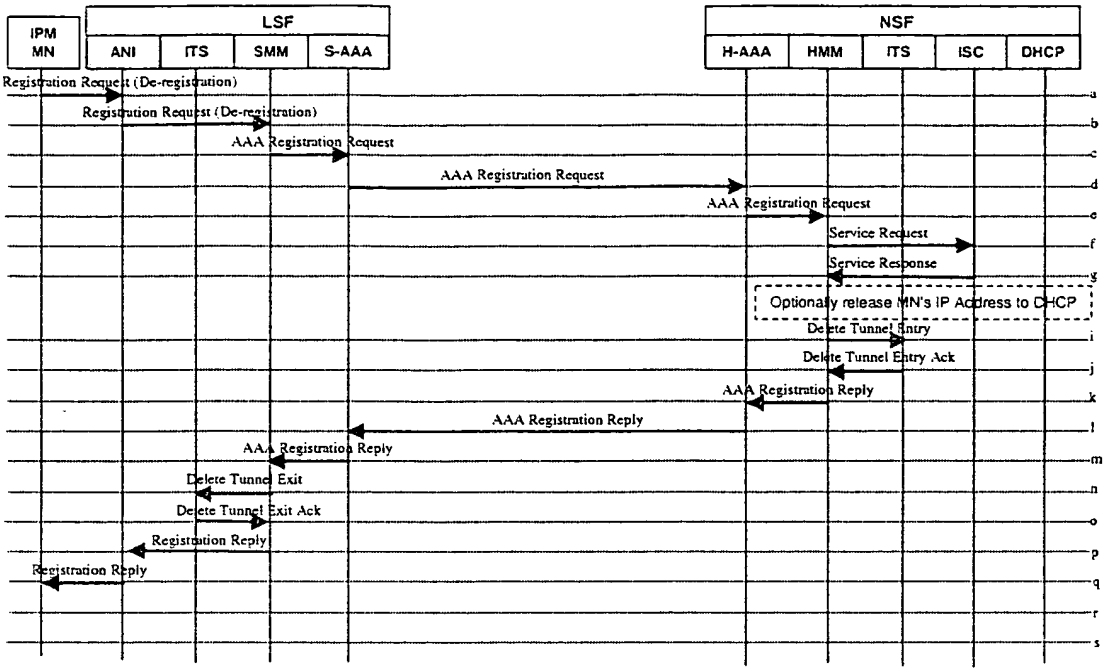
See Section 2.1.2.4

2.5.1.4 Registration Reply and Message Format

The Registration Reply Message is sent by the HMM to the IPM MN to indicate the result of the Registration Request Message sent.

See Section 2.1.2.10 for the message format exchanged between the HMM and the IPM MN.

2.6 IPM MN DE-REGISTERS FROM IPM LSF



IPM MN de-registers from IPM LSF

2.6.1 Registration Process

See Section 2.1.2

2.6.1.1 Registration Request and Message Format

See Section 2.1.2.1

2.6.1.2 AAA-Registration Request and Message Format

See Section 2.1.2.2

2.6.1.3 Service Request and Message Format

See Section 2.1.2.3

2.6.1.4 Service Response and Message Format

See Section 2.1.2.4

2.6.1.5 Delete Tunnel Entry and Message Format

The Delete Tunnel Entry Message is sent by the HMM to instruct ITS to delete a tunnel entry point.

The **message format** exchanged between the HMM and the ITS is as follows:

Code (16)	Message Length (16)
Identification (64)	
Extensions...	

- **Code** – 7, For Delete Tunnel Entry.
- **Message Length** – Length of the message including the header fields.
- **Identification** – Is used in matching requests and acknowledgements. The sender must ensure the identifier in a message is locally unique at any given time.

The Extensions used in the Delete Tunnel Entry Message are,

- **Host NAI Extension**
- **Mobile Node IP Address Extension**
- **User NAI Extension (Optional)**

and can be explained further in the Extension Section 4.

2.6.1.6 Delete Tunnel Entry Acknowledgement and Message Format

The Delete Tunnel Entry Acknowledgement Message is sent by the ITS to acknowledge the "Delete Tunnel Entry" Message. The identification field should be used for matching with the "Delete Tunnel Entry" Message.

The **message format** exchanged between the ITS and the HMM is as follows:

Code (16)	Message Length (16)
Identification (64)	
Extensions...	

- **Code** – 8, For Delete Tunnel Entry Acknowledgement.
- **Message Length** – Length of the message including the header fields.

- **Identification** – Is used in matching requests and acknowledgements. The sender must ensure the identifier in a message is locally unique at any given time.

The Extensions used in the Delete Tunnel Entry Acknowledgement Message are,

- **Host NAI Extension**
- **Result Code Extension**
- **Mobile Node IP Address Extension (Optional)**
- **User NAI Extension (Optional)**

and can be explained further in the Extension Section 4.

2.6.1.7 AAA-Registration Reply and Message Format

See Section 2.1.2.7

2.6.1.8 Delete Tunnel Exit and Message Format

The Delete Tunnel Exit Message is sent by the SMM to instruct the ITS to delete a tunnel exit point.

The **message format** exchanged between the SMM and the ITS is as follows:

Code (16)	Message Length (16)
Identification (64)	
Extensions...	

- **Code** – 9, For Delete Tunnel Exit.
- **Message Length** – Length of the message including the header fields.
- **Identification** – Is used in matching requests and acknowledgements. The sender must ensure the identifier in a message is locally unique at any given time.

The Extensions used in the Delete Tunnel Exit Message are,

- **Host NAI Extension**
- **Mobile Node IP Address Extension (Optional)**
- **User NAI Extension (Optional)**
- **Tunnel Exit IP Address Extension**

and can be explained further in the Extension Section 4.

2.6.1.9 Delete Tunnel Exit Acknowledgement and Message Format

The Delete Tunnel Exit Acknowledgement Message is sent by the ITS to acknowledge the "Delete Tunnel Exit" Message. The identification field should be used for matching with the "Delete Tunnel Exit" Message.

The **message format** exchanged between the ITS and the SMM is as follows:

Code (16)	Message Length (16)
Identification (64)	
Extensions...	

- **Code** – 10, For Delete Tunnel Exit Acknowledgement.
- **Message Length** – Length of the message including the header fields.
- **Identification** – Is used in matching requests and acknowledgements. The sender must ensure the identifier in a message is locally unique at any given time.

The Extensions used in the Delete Tunnel Exit Acknowledgement Message are,

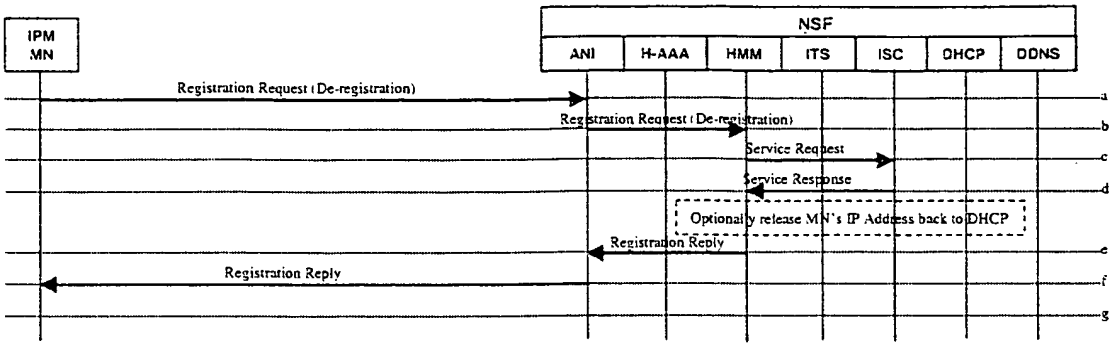
- **Host NAI Extension**
- **Result Code Extension**
- **Mobile Node IP Address Extension (Optional)**
- **User NAI Extension (Optional)**

and can be explained further in the Extension Section 4.

2.6.1.10 Registration Reply and Message Format

See Section 2.1.2.10

2.7 IPM MN DE-REGISTERS FROM IPM NSF



IPM MN de-registers from IPM NSF

2.7.1 Registration Process

See Section 2.1.2

2.7.1.1 Registration Request and Message Format

The Registration Request Message is sent by the IPM MN to the HMM to register for the service.

See Section 2.1.2.1 for the message format exchanged between the IPM MN and the HMM.

2.7.1.2 Service Request and Message Format

See Section 2.1.2.3

2.7.1.3 Service Response and Message Format

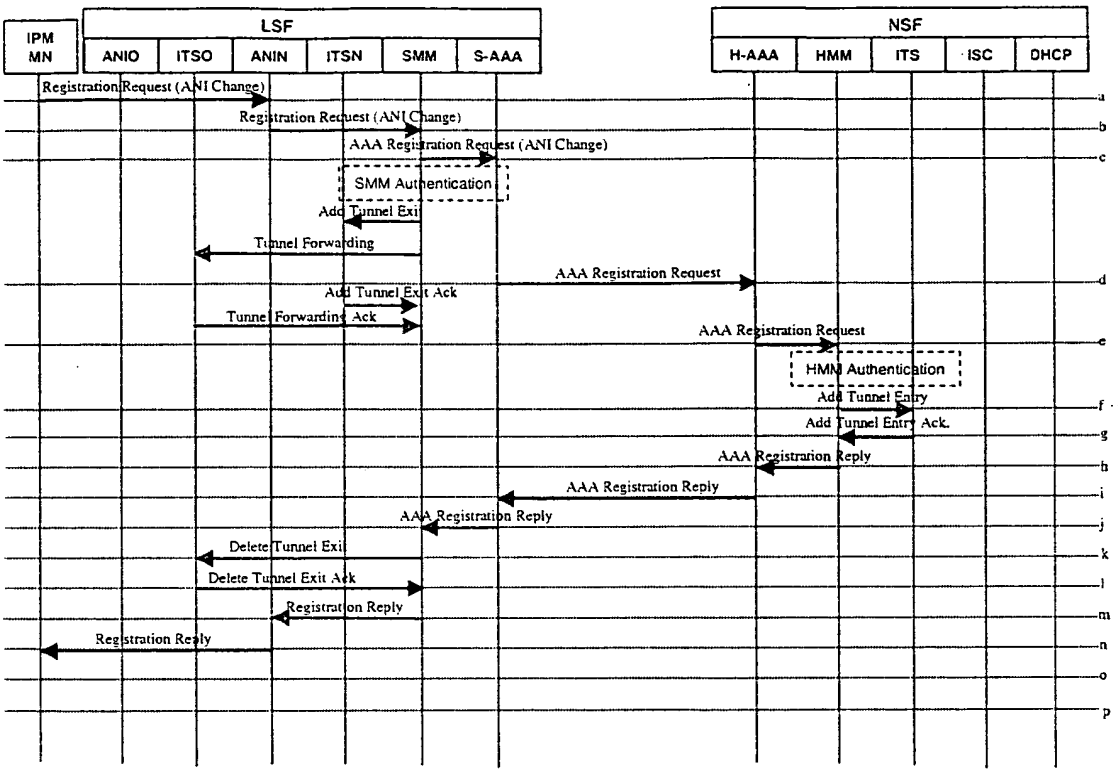
See Section 2.1.2.4

2.7.1.4 Registration Reply and Message Format

The Registration Reply Message is sent by the HMM to the IPM MN to indicate the result of the Registration Request Message sent.

See Section 2.1.2.10 for the message format exchanged between the HMM and the IPM MN.

2.8 IPM MN HANDOFFS FROM ANI TO ANI IN THE SAME SMM (DIFFERENT ITS)



IPM MN handoffs from ANI to ANI in the same SMM (different ITS)

2.8.1 Registration Process

See Section 2.1.2

2.8.1.1 Registration Request and Message Format

See Section 2.1.2.1

2.8.1.2 AAA-Registration Request and Message Format

See Section 2.1.2.2

2.8.1.3 Add Tunnel Exit and Message Format

See Section 2.1.2.8

2.8.1.4 Tunnel Forwarding and Message Format

The Tunnel Forwarding Message is sent by the SMM to instruct the ITS to set up a tunnel forwarding.

The **message format** exchanged between the SMM and the ITS is as follows:

Code (16)	Message Length (16)
Identification (64)	
Extensions...	

- **Code** – 5, For Tunnel Forwarding.
- **Message Length** – Length of the message including the header fields.
- **Identification** – Is used in matching requests and acknowledgements. The sender must ensure the identifier in a message is locally unique at any given time.

The Extensions used in the Tunnel Forwarding Message are,

- **Host NAI Extension**
- **Mobile Node IP Address Extension**
- **User NAI Extension (Optional)**
- **Lifetime Extension**
- **Tunnel Exit IP Address Extension**

and can be explained further in the Extension Section 4.

2.8.1.5 Add Tunnel Exit Acknowledgement and Message Format

See Section 2.1.2.9

2.8.1.6 Tunnel Forwarding Acknowledgement and Message Format

The Tunnel Forwarding Acknowledgement Message is sent by the ITS to acknowledge the "Tunnel Forwarding" message. The identification field should be used for matching with the "Tunnel Forwarding" message.

The **message format** exchanged between the ITS and the SMM is as follows:

Code (16)	Message Length (16)
Identification (64)	
Extensions...	

- **Code** – 6, For Tunnel Forwarding Acknowledgement.
- **Message Length** – Length of the message including the header fields.
- **Identification** – Is used in matching requests and acknowledgements. The sender must ensure the identifier in a message is locally unique at any given time.

The Extensions used in the Tunnel Forwarding Message are,

- **Host NAI Extension**
- **Mobile Node IP Address Extension**
- **User NAI Extension (Optional)**
- **Result Code Extension**

and can be explained further in the Extension Section 4.

2.8.1.7 Add Tunnel Entry and Message Format

See Section 2.1.2.5

2.8.1.8 Add Tunnel Entry Acknowledgement and Message Format

See Section 2.1.2.6

2.8.1.9 AAA-Registration Reply and Message Format

See Section 2.1.2.7

2.8.1.10 Delete Tunnel Exit and Message Format

See Section 2.6.1.8

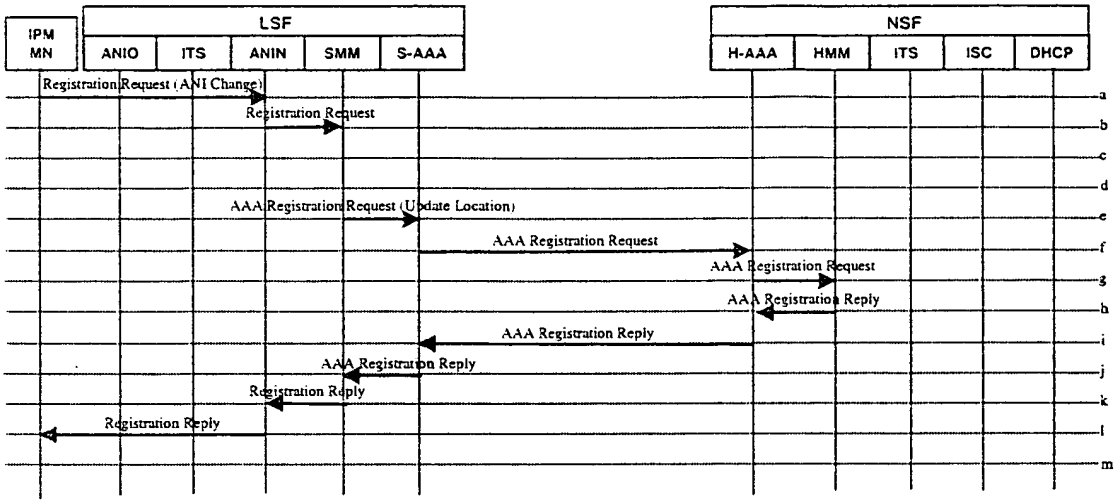
2.8.1.11 Delete Tunnel Exit Acknowledgement and Message Format

See Section 2.6.1.9

2.8.1.12 Registration Reply and Message Format

See Section 2.1.2.10

2.9 IPM MN HANDOFFS FROM ANI TO ANI IN THE SAME SMM (SAME ITS)



IPM MN handoffs from ANI to ANI in the same SMM (same ITS)

2.9.1 Registration Process

See Section 2.1.2

2.9.1.1 Registration Request and Message Format

See Section 2.1.2.1

2.9.1.2 AAA-Registration Request and Message Format

See Section 2.1.2.2

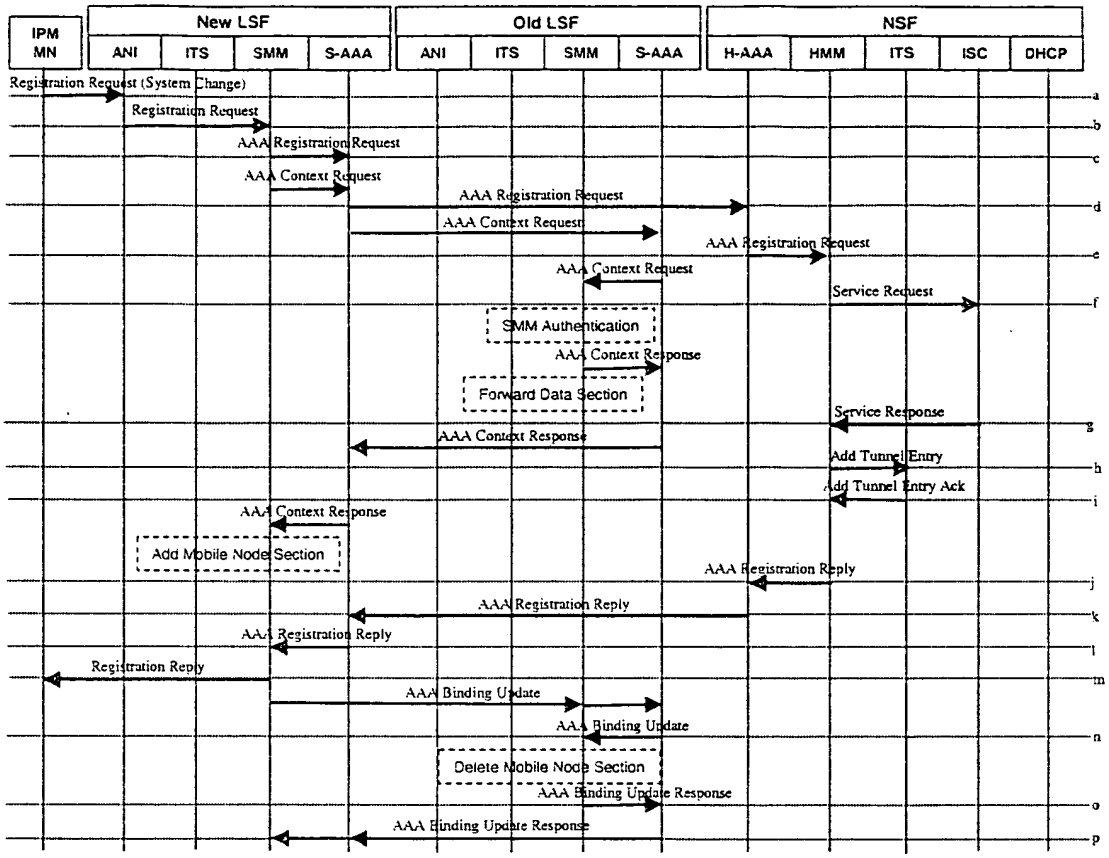
2.9.1.3 AAA-Registration Reply and Message Format

See Section 2.1.2.7

2.9.1.4 Registration Reply and Message Format

See Section 2.1.2.10

2.10 IPM MN HANDOFFS FROM SMM TO SMM



IPM MN handoffs from SMM to SMM

2.10.1 Registration Process

See Section 2.1.2

2.10.1.1 Registration Request and Message Format

See Section 2.1.2.1

2.10.1.2 AAA-Registration Request and Message Format

See Section 2.1.2.2

2.10.1.3 AAA-Context Request and Message Format

The AAA-Context-Request Message is sent by the current SMM of the User to the previous SMM to request the Context-Data of the User's session.

The **message format** exchanged between the current SMM and the previous SMM is as follows:

AAA-Context-Request	<DIAMETER Header>
	<Command-Code AVP = 339>
	<Destination-NAI AVP>
	<Host-Name AVP>
	<User-Name AVP>
	<IPM-Context-Request-Type AVP>
	<IPM-Care-of-Address AVP>

The AAA-Context-Request Message is of the format of DIAMETER. The current SMM of the MN sends this message to previous SMM, to request for the context of the user's data and also to request to forward the data to the current COA. The current SMM sends the IPM-Registration-Request AVP that encapsulates the incoming IPM-Registration-Request Message for the previous SMM to authenticate before forwarding the data. The IPM-Context-Request-Type AVP informs the previous SMM what kind of action is requested.

The AVPs that can optionally be used in the AAA-Context-Request Message are,

- **IPM-Registration-Request AVP**
- **IPM-SMM-NAI AVP**
- **Proxy-State AVP**
- **Time AVP**
- **Nonce AVP**
- **Integrity-Check-Value AVP**

and can be explained further in the AVPs Section 5.

2.10.1.4 Service Request and Message Format

See Section 2.1.2.3

2.10.1.5 AAA-Context Response and Message Format

The AAA-Context-Response Message is sent by previous SMM of the User to the current SMM in response to the AAA-Context-Request Message.

The **message format** exchanged between the previous SMM and the current SMM is as follows:

AAA-Context-Response	<DIAMETER Header>
	<Command-Code AVP = 340>
	<Destination-NAI AVP>
	<Host-Name AVP>
	<User-Name AVP>
	<Result-Code AVP>

The AAA-Context-Response Message is of the format of DIAMETER. The previous SMM of the MN sends this message to current SMM, to response to the AAA-Context-Request Message. The successful message must have IPM-Context-Data AVP in the message.

The AVPs that can optionally be used in the AAA-Context-Response Message are,

- **IPM-Context-Data AVP**
- **Proxy-State AVP**
- **Time AVP**
- **Nonce AVP**
- **Integrity-Check-Value AVP**

and can be explained further in the AVPs Section 5.

2.10.1.6 Service Response and Message Format

See Section 2.1.2.4

2.10.1.7 Add Tunnel Entry and Message Format

See Section 2.1.2.5

2.10.1.8 Add Tunnel Entry Acknowledgement and Message Format

See Section 2.1.2.6

2.10.1.9 AAA-Registration Reply and Message Format

See Section 2.1.2.7

2.10.1.10 Registration Reply and Message Format

See Section 2.1.2.10

2.10.1.11 AAA-Binding-Update Request and Message Format

The AAA-Binding-Update Request Message is sent by the current SMM of the User to the previous SMM to complete the hand-off of the User's session.

The **message format** exchanged between the current SMM and the previous SMM is as follows:

AAA-Binding-Update Request	<DIAMETER Header>
	<Command-Code AVP = 341>
	<Destination-NAI AVP>
	<Host-Name AVP>
	<User-Name AVP>
	<IPM-Client-Address AVP>
	<IPM-Care-of-Address AVP>

The AAA-Binding-Update Request Message is of the format of DIAMETER. The current SMM of the MN sends this message to the previous SMM, to complete the hand-off of the User's session and clean up of the resources that are allocated for the user.

The AVPs that can optionally be used in the AAA-Binding-Update Request Message are,

- IPM-SMM-NAI AVP
- Proxy-State AVP
- Time AVP
- Nonce AVP
- Integrity-Check-Value AVP

and can be explained further in the AVPs Section 5.

2.10.1.12 AAA-Binding Update Response and Message Format

The AAA-Binding-Update Response Message is sent by the previous SMM of the User to the current SMM in response to the AAA-Binding-Update Request Message.

The **message format** exchanged between the previous SMM and the current SMM is as follows:

AAA-Binding-Update Response	<DIAMETER Header>
	<Command-Code AVP = 342>
	<Destination-NAI AVP>
	<Host-Name AVP>
	<User-Name AVP>
	<Result-Code AVP>

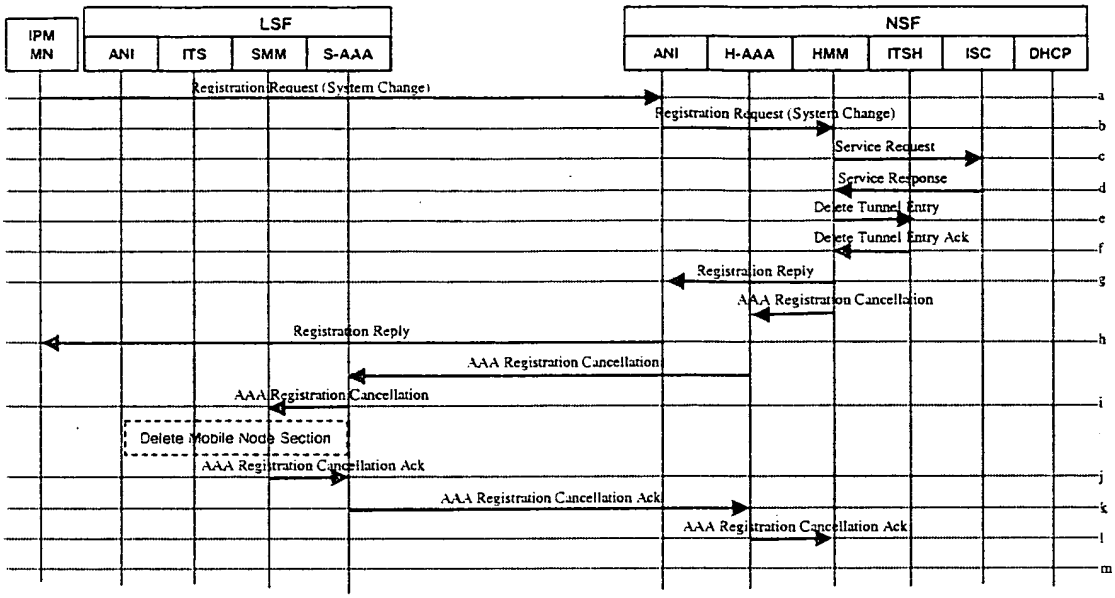
The AAA-Binding-Update Response Message is of the format of DIAMETER. The previous SMM of the MN sends this message to the current SMM, in response to the AAA-Binding-Update Request Message. The successful message completes the hand-off of the MN from SMM to SMM.

The AVPs that can optionally be used in the AAA-Binding-Update Response Message are,

- **Proxy-State AVP**
- **Time AVP**
- **Nonce AVP**
- **Integrity-Check-Value AVP**

and can be explained further in the AVPs Section 5.

2.11 IPM MN HANDOFFS LSF TO NSF



IPM MN handoffs from LSF to NSF (Home ANI)

2.11.1 Registration Process

See Section 2.1.2

2.11.1.1 Registration Request and Message Format

The Registration Request Message is sent by the IPM MN to the HMM to register for the service.

See Section 2.1.2.1 for the message format exchanged between the IPM MN and the HMM.

2.11.1.2 Service Request and Message Format

See Section 2.1.2.3

2.11.1.3 Service Response and Message Format

See Section 2.1.2.4

2.11.1.4 Delete Tunnel Entry and Message Format

See Section 2.6.1.5

2.11.1.5 Delete Tunnel Entry Acknowledgement and Message Format

See Section 2.6.1.6

2.11.1.6 Registration Reply and Message Format

The Registration Reply Message is sent by the HMM to the IPM MN to indicate the result of the Registration Request Message sent.

See Section 2.1.2.10 for the message format exchanged between the HMM and the IPM MN.

2.11.1.7 AAA-Registration Cancellation and Message Format

The AAA-Registration Cancellation Message is sent by the HMM to the SMM to cancel the existing User's registration at the visiting system.

AAA-Registration Cancellation	<DIAMETER Header>
	<Command-Code AVP = 337>
	<Destination-NAI AVP>
	<Host-Name AVP>
	<User-Name AVP>
	<IPM-Registration-Cancellation-Reason AVP>

The AAA-Registration Cancellation Message is of the format of DIAMETER. The HMM sends the message to the SMM with at least the mandatory fields to cancel the registration of the user. The IPM-Registration-Cancellation-Reason AVP indicates the reason for the cancellation of the registration.

The AVPs that can optionally be used in the AAA-Registration Cancellation Message are,

- **IPM-Client-Address AVP**
- **Proxy-State AVP**
- **Time AVP**
- **Nonce AVP**
- **Integrity-Check-Value AVP**

and can be explained further in the AVPs Section 5.

2.11.1.8 AAA-Registration Cancellation Acknowledgement and Message Format

The AAA-Registration Cancellation Acknowledgement Message is sent by the SMM to the HMM in response to the AAA-Registration Cancellation.

The **message format** exchanged between the SMM and the HMM is as follows:

AAA-Registration Cancellation Acknowledgement	<DIAMETER Header>
	<Command-Code AVP = 338>
	<Destination-NAI AVP>
	<Host-Name AVP>
	<User-Name AVP>
	<Result-Code AVP>

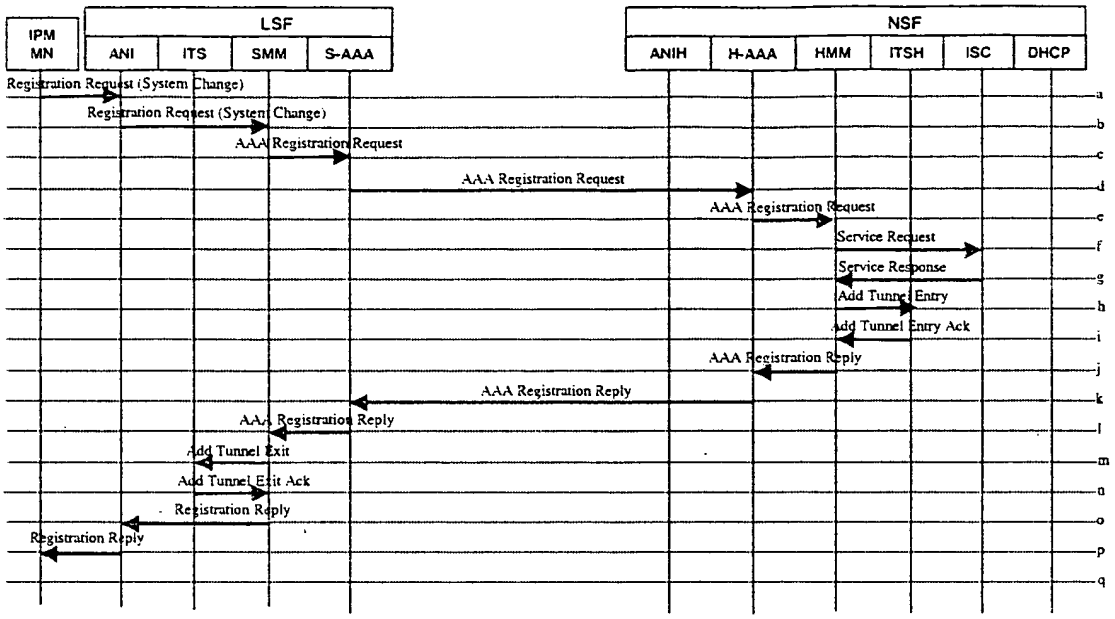
The AAA-Registration Cancellation Acknowledgement Message is of the format of DIAMETER. The SMM sends the message to the HMM with at least the mandatory fields. The Response-Code AVP indicates the failure or success of the AAA-Registration Cancellation Message.

The AVPs that can optionally be used in the AAA-Registration Cancellation Acknowledgement Message are,

- **Proxy-State AVP**
- **Time AVP**
- **Nonce AVP**
- **Integrity-Check-Value AVP**

and can be explained further in the AVPs Section 5.

2.12 IPM MN HANDOFFS NSF (HOME ANI) TO LSF



IPM MN handoffs from NSF (Home ANI) to LSF

2.12.1 Registration Process

See Section 2.1.2

2.12.1.1 Registration Request and Message Format

See Section 2.1.2.1

2.12.1.2 AAA-Registration Request and Message Format

See Section 2.1.2.2

2.12.1.3 Service Request and Message Format

See Section 2.1.2.3

2.12.1.4 Service Response and Message Format

See Section 2.1.2.4

2.12.1.5 Add Tunnel Entry and Message Format

See Section 2.1.2.5

2.12.1.6 Add Tunnel Entry Acknowledgement and Message Format

See Section 2.1.2.6

2.12.1.7 AAA-Registration Reply and Message Format

See Section 2.1.2.7

2.12.1.8 Add Tunnel Exit and Message Format

See Section 2.1.2.8

2.12.1.9 Add Tunnel Exit Acknowledgement and Message Format

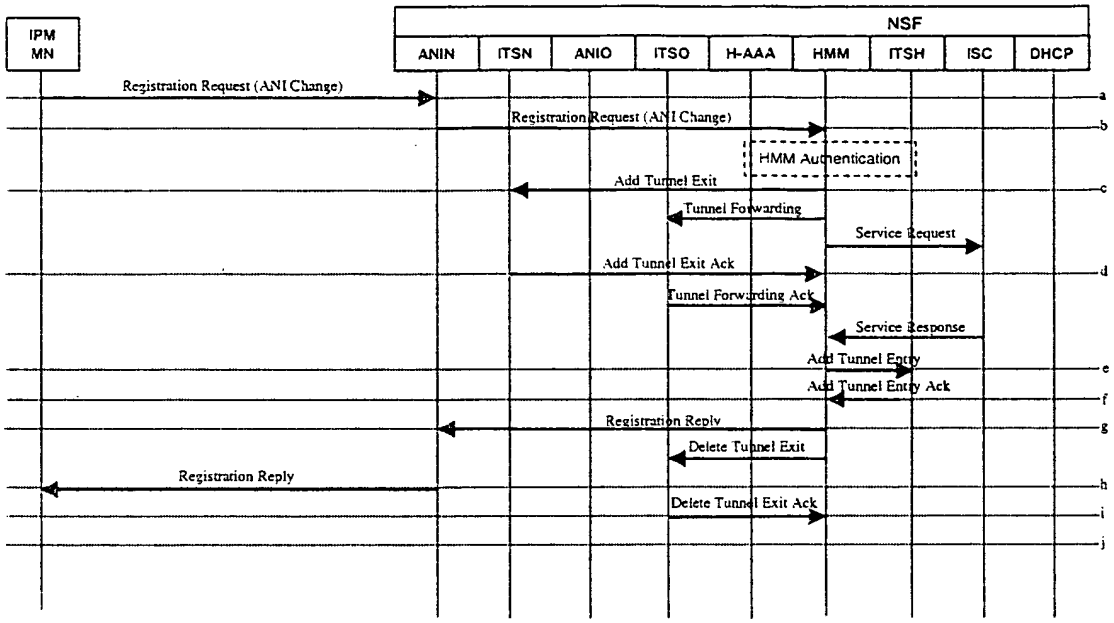
See Section 2.1.2.9

2.12.1.10 Registration Reply and Message Format

See Section 2.1.2.10

DRAFT - 25 Feb 2000

2.13 IPM MN HANDOFFS FROM FOREIGN ANI TO FOREIGN ANI IN THE SAME NSF



IPM MN handoffs from foreign ANI to foreign ANI in the same NSF

2.13.1 Registration Process

See Section 2.1.2

2.13.1.1 Registration Request and Message Format

See Section 2.1.2.1

2.13.1.2 Add Tunnel Exit and Message Format

See Section 2.1.2.8

2.13.1.3 Tunnel Forwarding and Message Format

See Section 2.8.1.4

2.13.1.4 Service Request and Message Format

See Section 2.1.2.3

2.13.1.5 Add Tunnel Exit Acknowledgement and Message Format

See Section 2.1.2.9

2.13.1.6 Tunnel Forwarding Acknowledgement and Message Format

See Section 2.8.1.6

2.13.1.7 Service Response and Message Format

See Section 2.1.2.4

2.13.1.8 Add Tunnel Entry and Message Format

See Section 2.1.2.5

2.13.1.9 Add Tunnel Entry Acknowledgement and Message Format

See Section 2.1.2.6

2.13.1.10 Registration Reply and Message Format

See Section 2.1.2.10

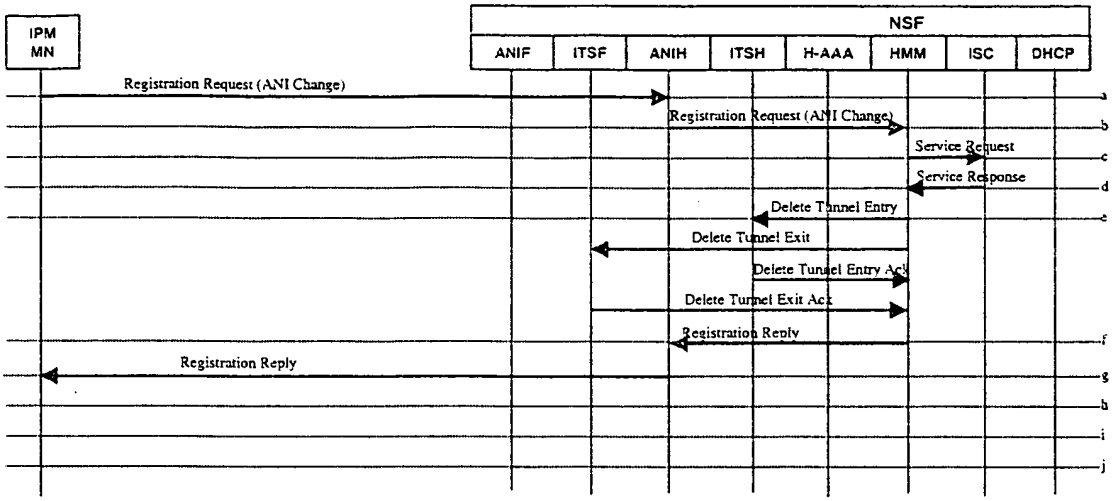
2.13.1.11 Delete Tunnel Exit and Message Format

See Section 2.6.1.8

2.13.1.12 Delete Tunnel Exit Acknowledgement and Message Format

See Section 2.6.1.9

2.14 IPM MN HANDOFFS FROM FOREIGN ANI TO FOREIGN ANI IN THE SAME NSF



IPM MN handoffs from foreign ANI to home ANI in the same NSF

2.14.1 Registration Process

See Section 2.1.2

2.14.1.1 Registration Request and Message Format

See Section 2.1.2.1

2.14.1.2 Service Request and Message Format

See Section 2.1.2.3

2.14.1.3 Service Response and Message Format

See Section 2.1.2.4

2.14.1.4 Add Tunnel Entry and Message Format

See Section 2.1.2.5

2.14.1.5 Add Tunnel Exit and Message Format

See Section 2.1.2.8

2.14.1.6 Add Tunnel Entry Acknowledgement and Message Format

See Section 2.1.2.6

2.14.1.7 Add Tunnel Exit Acknowledgement and Message Format

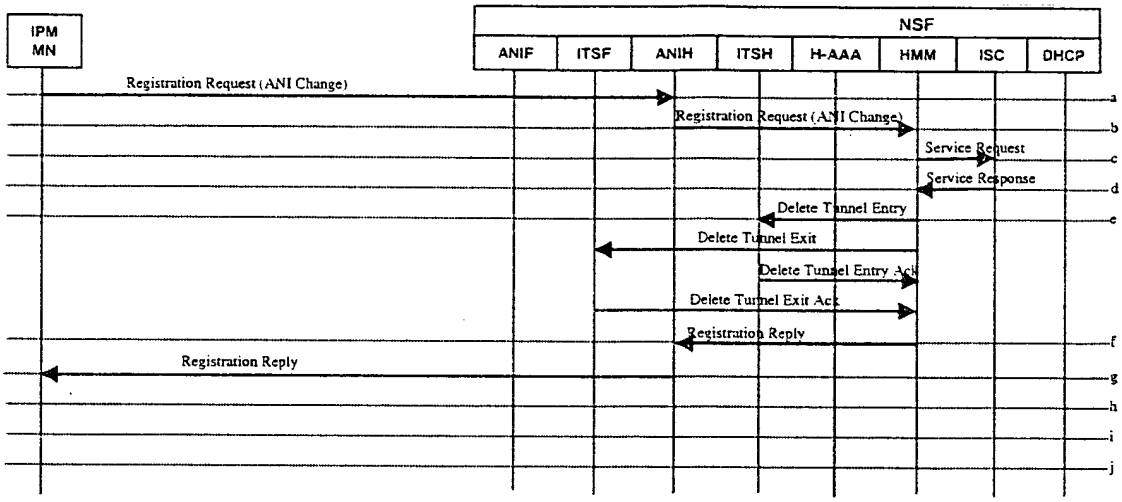
See Section 2.1.2.9

2.14.1.8 Registration Reply and Message Format

See Section 2.1.2.10

Exhibit 2005, Page 51 of 130

2.15 IPM MN HANDOFFS FROM FOREIGN ANI TO HOME ANI IN THE SAME NSF



IPM MN handoffs from foreign ANI to home ANI in the same NSF

2.15.1 Registration Process

See Section 2.1.2

2.15.1.1 Registration Request and Message Format

See Section 2.1.2.1

2.15.1.2 Service Request and Message Format

See Section 2.1.2.3

2.15.1.3 Service Response and Message Format

See Section 2.1.2.4

2.15.1.4 Delete Tunnel Entry and Message Format

See Section 2.6.1.5

2.15.1.5 Delete Tunnel Exit and Message Format

See Section 2.6.1.8

2.15.1.6 Delete Tunnel Entry Acknowledgement and Message Format

See Section 2.6.1.6

2.15.1.7 Delete Tunnel Exit Acknowledgement and Message Format

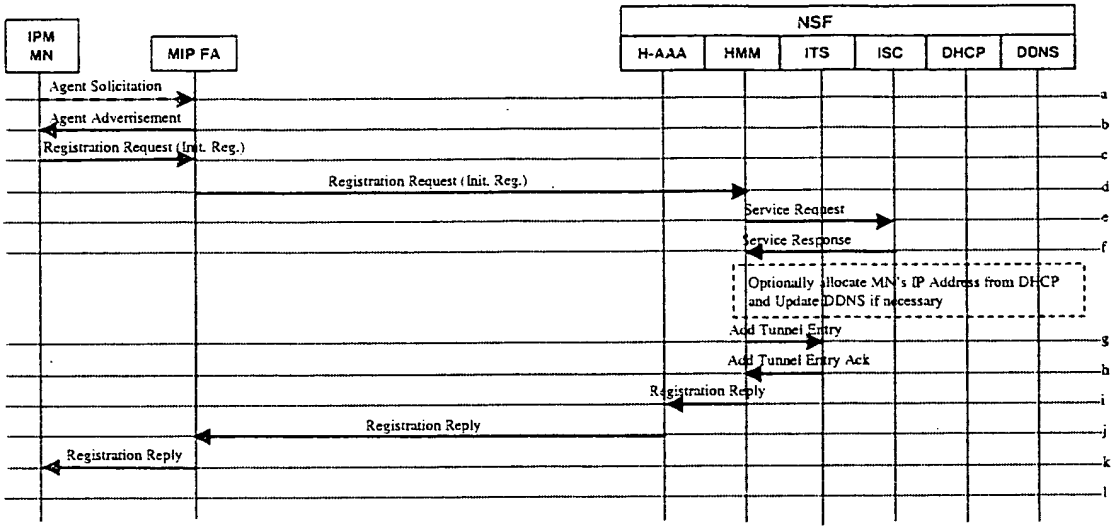
See Section 2.6.1.9

2.15.1.8 Registration Reply and Message Format

See Section 2.1.2.10

3. INTERWORKING MESSAGE FLOWS IPM-MIP

3.1 IPM MN REGISTERS FROM MIP FA



IPM MN registers from MIP FA

3.1.1 Agent Discovery Process

Agent Discovery is the method by which a mobile node determines whether it is currently connected to its home network or to a foreign network, and by which a mobile node can detect when it has moved from one network to another. Home agents and foreign agents may advertise their availability on each link for which they provide service. A newly arrived mobile node can send a solicitation on the link to learn if any prospective agents are present. The Agent Discovery Process is primarily handled through Agent Solicitation and Agent Advertisement.

3.1.1.1 Agent Solicitation and Message Format

Agent Solicitation is the broadcast/multicast message sent by the IPM MN to detect a Service Provider in the event that the IPM MN has not received an Advertising Agent message.

The **message format** exchanged between the IPM MN and the MIP FA is as follows:

Type	Code	Checksum
Reserved		

- **Source Address** – An Mobile IP address belonging to the interface from which this message is sent, or 0. This is part of the standard heading.
- **Destination Address** – The configured Solicitation Address. This is part of the standard heading.
- **Type** – 10
- **Code** – 0
- **Checksum** – The 16-bit one's complement of the one's complement sum of the ICMP message, starting with the ICMP Type. For computing the checksum, the Checksum field is set to 0.
- **Reserved** – Sent as 0; ignored on reception.

There are no Extensions for Agent Solicitation.

3.1.1.2 Agent Advertisement and Message Format

Agent Advertisement are messages sent periodically, either as a broadcast or multicast for the visiting IPM MN to recognize the availability of service and to keep track of their point of attachment.

The **message format** exchanged between the MIP FA and the IPM MN is as follows:

Type	Code	Checksum
Num Addrs	Addr Entry Size	Lifetime
Router Address [1]		
Preference Level [1]		
Router Address [2]		
Preference Level [2]		

- **Source Address** – An IP address belonging to the interface from which this message is sent. This is part of the of the standard heading.
- **Destination Address** – The configured Advertisement Address or the IP address of a neighboring host. This is part of the of the standard heading.
- **Type** – 9
- **Code** – 0
- **Checksum** – The 16-bit one's complement of the one's complement sum of the ICMP message, starting with the ICMP Type. For computing the checksum, the checksum field is set to 0.
- **Num Addrs** – The number of router addresses advertised in this message.
- **Addr Entry Size** – The number of 32-bit words of information per each router address (2, in the version of the protocol described here).
- **Lifetime** – The maximum number of seconds that the router addresses may be considered valid.

- **Router Address [i], i = 1..Num Addrs** – The sending router's IP address(es) on the interface from which this message is sent.
- **Preference Level [i], i = 1..Num Addrs** – The preferability of each router address [i] as a default router address, relative to other router addresses on the same subnet. A signed, two-complement value; higher values mean more preferable.

The Extensions that can be used in Agent Advertisement Message are,

- **Mobility Agent Advertisement Extension**
- **Prefix-Lengths Extension (Optional)**
- **One-Byte Padding Extension (Optional)**

and can be explained further in the Extension Section 4.

3.1.2 Registration Process

The purpose of registration is for the IPM MN to inform the HMM of the NSF (Network Serving Function) of its current location to which data packets can be forwarded to the IPM MN. The Registration process also includes the authenticating and authorizing of the MIP MN to have access to the visited network or LSF (Local Serving Function).

3.1.2.1 Registration Request and Message Format

The Registration Request Message is sent by the IPM MN to the HMM to register for the service. The Registration process also includes the authenticating and authorizing of the IPM MN to have access to the visited network or FA.

The **message format** exchanged between the IPM MN and the HMM is as follows:

Type (8)	Flags (8)	Lifetime (16)
Home Address (32)		
Home Agent (32)		
Care-of-Address (32)		
Identification (64)		

- **Source Address** – An IP address of the MN. This is part of the standard heading.
- **Destination Address** – The COA within the ANI component. This is part of the standard heading.
- **Type** – The type of the message is "0", which is the Registration Request Message.
- **Flags** – The flags filed are the same as RFC2002.
- **Lifetime** – The lifetime requested by MN from the HMM or Home.

- **Home Address** – The IP address of the Mobile Node.
- **Home Agent** – The Home Agent's address of the Mobile Node.
- **Care-of-Address** – The Care-of-Address of the Mobile Node.
- **Identification** – The identification, to provide replay protection.

The Extensions used in the Registration Request are,

- **Mobile-Home Authentication Extension**
- **Mobile-Foreign Authentication Extension (Optional)**
- **Foreign-Home Authentication Extension (Optional)**

and can be explained further in the Extension Section 4.

3.1.2.2 Service Request and Message Format

The Service Request Message is sent from the HMM to the ISC (IPM Security Center) to authenticate a user or message, generate, renew, or delete session secret keys. It also can be sent from the PPS Manager to the ISC to generate or construct the IPMC.

The **message format** exchanged between the HMM and the ISC is as follows:

Type	Sub-Type	Payload Length
Identification		
User NAI		

- **Type** – USER_SERVICE_REQUEST_MSG.
- **Sub-Type** – 0.
- **Payload Length** – Length of the message payload including all the extensions.
- **Identification** – A 64-bit number used for matching User Service Request Messages with User Service Reply messages, and for protecting against replay attacks of User Service Request messages.
- **User NAI** – In phase I, this Extension has the user NAI and in the future will have an index which will be used to index the user data in the UDS.

The Extensions used in the Service Request Message are,

- **User Authentication Information Extension**
- **Control Message Authentication Extension**
- **Session Key Allocation Extension 0..N**
- **Session Key Lifetime Renewal Extension 0..N**
- **Session Key Delete Extension 0..N**

and can be explained further in the Extension Section 4.

3.1.2.3 Service Response and Message Format

The Service Response Message is sent from the ISC (IPM Security Center) to the HMM in response to a Service Request Message.

The **message format** exchanged between the ISC and the HMM is as follows:

Type	Sub-Type	Payload Length
Code		
Identification		
User NAI		

- **Type** – USER_SERVICE_REPLY_MSG.
- **Sub-Type** – 0.
- **Payload Length** – Length of the message payload including all the extensions.
- **Code** – The following are the hex values of the defined codes:
  - 00000001 User Authenticated successfully.
  - 00000002 All required keys have been allocated.
  - 00000003 Some keys have been allocated.
  - 00000004 User Authentication failed.
  - 00000005 Key Lifetime Renewal is completely honoured.
  - 00000006 Key Lifetime Renewal is partially honoured.
  - 00000007 User Account is created successfully.
  - 00000008 User is deleted successfully.
- **Identification** – A 64-bit number used for matching User Service Request Messages with User Service Reply Messages, and for protecting against replay attacks of User Service Request Messages.
- **User NAI** – In phase I, this Extension has the user NAI and in the future will have an index which will be used to index the user data in the UDS.

The Extensions used in the Service Response Message are,

- **Control Message Authentication Extension**
- **Session Key Allocation Extension 0..N**
- **Session Key Lifetime Renewal Extension 0..N**
- **Session Key Delete Extension 0..N**

and can be explained further in the Extension Section 4.

3.1.2.4 Add Tunnel Entry and Message Format

The Add Tunnel Entry Message is sent by the HMM to instruct the ITS to set up a tunnel entry point.

The **message format** exchanged between the HMM and the ITS is as follows:

Code (16)	Message Length (16)
Identification (64)	
Extensions...	

- **Code** – 1, For Add Tunnel Entry.
- **Message Length** – Length of the message including the header fields.
- **Identification** – Is used in matching requests and acknowledgements. The sender must ensure the identifier in a message is locally unique at any given time.

The Extensions used in the Add Tunnel Entry Message are,

- **Host NAI Extension**
- **Flag Extension**
- **Lifetime Extension**
- **Mobile Node IP Address Extension**
- **User NAI Extension (Optional)**
- **Tunnel Entry IP Address Extension**

and can be explained further in the Extension Section 4.

3.1.2.5 Add Tunnel Entry Acknowledgement and Message Format

The Add Tunnel Entry Acknowledgement Message is sent by the ITS to acknowledge the "Add Tunnel Entry" Message.

The **message format** exchanged between the ITS and the HMM is as follows:

Code (16)	Message Length (16)
Identification (64)	
Extensions...	

- **Code** – 2, For Add Tunnel Entry Acknowledgement.
- **Message Length** – Length of the message including the header fields.

- **Identification** – Is used in matching requests and acknowledgements. The sender must ensure the identifier in a message is locally unique at any given time.

The Extensions used in the Add Tunnel Entry Message are,

- **Host NAI Extension**
- **Result Code Extension**
- **Mobile Node IP Address Extension (Optional)**
- **User NAI Extension (Optional)**

and can be explained further in the Extension Section 4.

3.1.2.6 Registration Reply and Message Format

The Registration Reply Message is sent by the HMM to the IPM MN to indicate the result of the Registration Request Message sent.

The **message format** exchanged between the HMM and the IPM MN is as follows:

Type (8)	Code (8)	Lifetime
Home Address (32)		
Home Agent (32)		
Identification (64)		

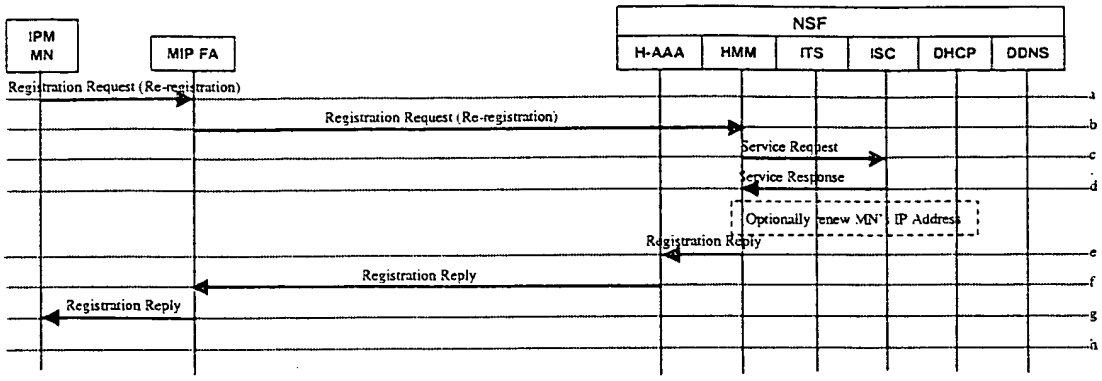
- **Type** – The type of the message is 3, which is the Registration Request Message.
- **Code** – All the existing MIP Response codes, this field is being extended to include IPM specific items.
- **Lifetime** – The Home lifetime for the registration.
- **Home Address** – The IP address of the Mobile Node.
- **Home Agent** – The Home Agent's address of the Mobile Node.
- **Identification** – The identification, to provide replay protection.

The Extensions used in the Registration Reply Message are,

- **Mobile-Home Authentication Extension**
- **Foreign-Home Authentication Extension (Optional)**
- **Mobile-Foreign Authentication Extension (Optional)**

and can be explained further in the Extension Section 4.

3.2 IPM MN RE-REGISTERS FROM MIP FA



IPM MN re-registers from MIP FA

3.2.1 Registration Process

See Section 3.1.2

3.2.1.1 Registration Request and Message Format

See Section 3.1.2.1

3.2.1.2 Service Request and Message Format

See Section 3.1.2.2

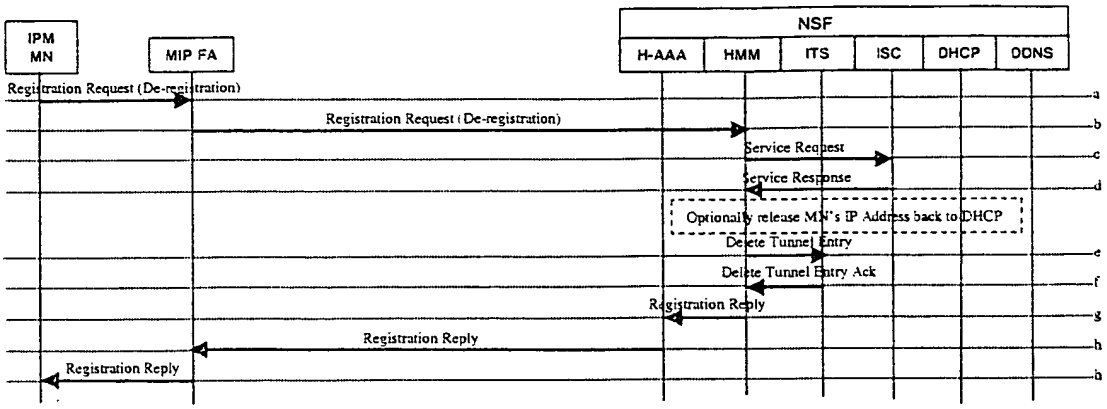
3.2.1.3 Service Response and Message Format

See Section 3.1.2.3

3.2.1.4 Registration Reply and Message Format

See Section 3.1.2.6

3.3 IPM MN DE-REGISTERS FROM MIP FA



IPM MN de-registers from MIP FA

3.3.1 Registration Process

See Section 3.1.2

3.3.1.1 Registration Request and Message Format

See Section 3.1.2.1

3.3.1.2 Service Request and Message Format

See Section 3.1.2.2

3.3.1.3 Service Response and Message Format

See Section 3.1.2.3

3.3.1.4 Delete Tunnel Entry and Message Format

The Delete Tunnel Entry Message is sent by the HMM to instruct the ITS to delete a tunnel entry point.

The **message format** exchanged between the HMM and the ITS is as follows:

Code (16)	Message Length (16)
Identification (64)	
Extensions...	

- **Code** – 7, For Delete Tunnel Entry.

- **Message Length** – Length of the message including the header fields.
- **Identification** – Is used in matching requests and acknowledgements. The sender must ensure the identifier in a message is locally unique at any given time.

The Extensions used in the Delete Tunnel Entry Message are,

- **Host NAI Extension**
- **Mobile Node IP Address Extension**
- **User NAI Extension (Optional)**

and can be explained further in the Extension Section 4.

3.3.1.5 Delete Tunnel Entry Acknowledgement and Message Format

The Delete Tunnel Entry Acknowledgement Message is sent by the ITS to acknowledge the "Delete Tunnel Entry" Message. The identification field should be used for matching with the "Delete Tunnel Entry" Message.

The **message format** exchanged between the ITS and the HMM is as follows:

Code (16)	Message Length (16)
Identification (64)	
Extensions...	

- **Code** – 8, For Delete Tunnel Entry Acknowledgement.
- **Message Length** – Length of the message including the header fields.
- **Identification** – Is used in matching requests and acknowledgements. The sender must ensure the identifier in a message is locally unique at any given time.

The Extensions used in the Delete Tunnel Entry Acknowledgement Message are,

- **Host NAI Extension**
- **Result Code Extension**
- **Mobile Node IP Address Extension (Optional)**
- **User NAI Extension (Optional)**

and can be explained further in the Extension Section 4.

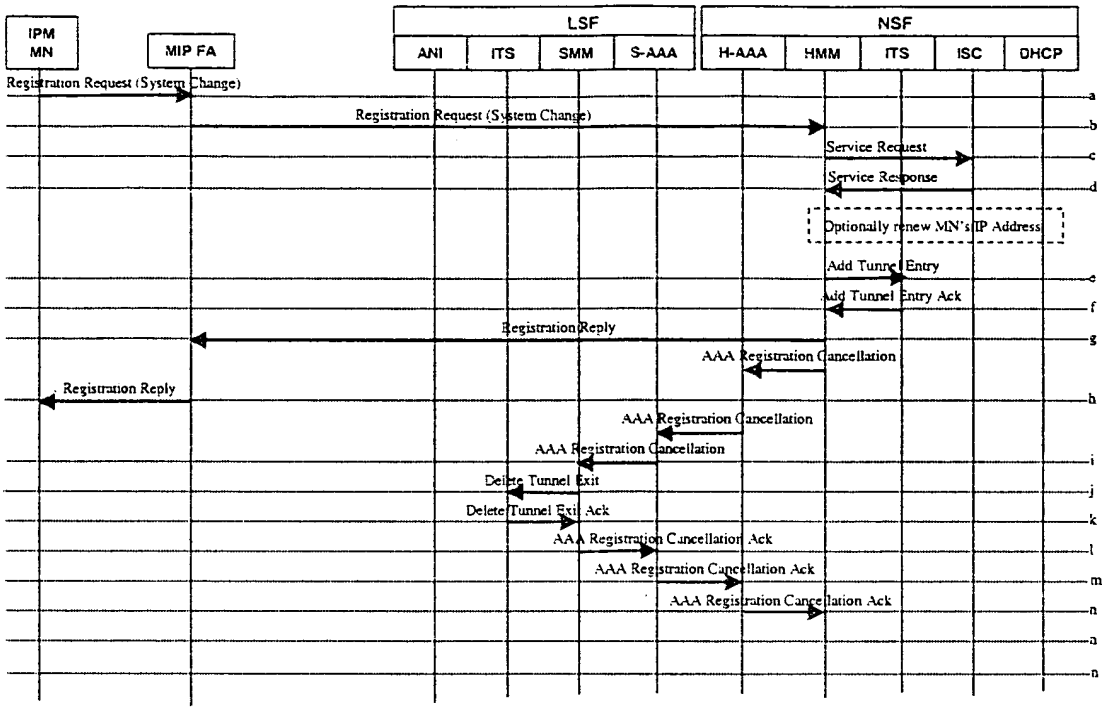
3.3.1.6 Registration Reply and Message Format

See Section 3.1.2.6

This Page Blank (uspto)

EXHIBIT 2005

3.4 IPM MN HANDOFFS FROM IPM ANI TO FA (NO SMOOTH HANDOFF)



IPM MN handoff from IPM ANI To FA (FA does not support smooth handoff)

3.4.1 Registration Process

See Section 3.1.2

3.4.1.1 Registration Request and Message Format

See Section 3.1.2.1

3.4.1.2 Service Request and Message Format

See Section 3.1.2.2

3.4.1.3 Service Response and Message Format

See Section 3.1.2.3

3.4.1.4 Add Tunnel Entry and Message Format

See Section 3.1.2.4

3.4.1.5 Add Tunnel Entry Acknowledgement and Message Format

See Section 3.1.2.5

3.4.1.6 Registration Reply and Message Format

See Section 3.1.2.6

3.4.1.7 AAA-Registration Cancellation and Message Format

The AAA-Registration Cancellation Message is sent by the HMM to the SMM to cancel the existing User's registration at the visiting system.

AAA-Registration Cancellation	<DIAMETER Header>
	<Command-Code AVP = 337>
	<Destination-NAI AVP>
	<Host-Name AVP>
	<User-Name AVP>
	<IPM-Registration-Cancellation-Reason AVP>

The AAA-Registration Cancellation Message is of the format of DIAMETER. The HMM sends the message to the SMM with at least the mandatory fields to cancel the registration of the user. The IPM-Registration-Cancellation-Reason AVP indicates the reason for the cancellation of the registration.

The AVPs that can optionally be used in the AAA-Registration Cancellation Message are,

- **IPM-Client-Address AVP**
- **Proxy-State AVP**
- **Time AVP**
- **Nonce AVP**
- **Integrity-Check-Value AVP**

and can be explained further in the AVPs Section 5.

3.4.1.8 Delete Tunnel Exit and Message Format

The Delete Tunnel Exit Message is sent by the SMM to instruct the ITS to delete a tunnel exit point.

The **message format** exchanged between the SMM and the ITS is as follows:

Code (16)	Message Length (16)
Identification (64)	
Extensions...	

- **Code** – 9, For Delete Tunnel Exit.
- **Message Length** – Length of the message including the header fields.
- **Identification** – Is used in matching requests and acknowledgements. The sender must ensure the identifier in a message is locally unique at any given time.

The Extensions used in the Delete Tunnel Exit Message are,

- **Host NAI Extension**
- **Mobile Node IP Address Extension (Optional)**
- **User NAI Extension (Optional)**
- **Tunnel Exit IP Address Extension**

and can be explained further in the Extension Section 4.

3.4.1.9 Delete Tunnel Exit Acknowledgement and Message Format

The Delete Tunnel Exit Acknowledgement Message is sent by the ITS to acknowledge the "Delete Tunnel Exit" Message. The identification field should be used for matching with the "Delete Tunnel Exit" Message.

The **message format** exchanged between the ITS and the SMM is as follows:

Code (16)	Message Length (16)
Identification (64)	
Extensions...	

- **Code** – 10, For Delete Tunnel Exit Acknowledgement.
- **Message Length** – Length of the message including the header fields.
- **Identification** – Is used in matching requests and acknowledgements. The sender must ensure the identifier in a message is locally unique at any given time.

The Extensions used in the Delete Tunnel Exit Acknowledgement Message are,

- **Host NAI Extension**
- **Result Code Extension**

- **Mobile Node IP Address Extension (Optional)**
- **User NAI Extension (Optional)**

and can be explained further in the Extension Section 4.

3.4.1.10 AAA-Registration Cancellation Acknowledgement and Message Format

The AAA-Registration Cancellation Acknowledgement Message is sent by the SMM to the HMM in response to the AAA-Registration Cancellation Message.

The **message format** exchanged between the SMM and the HMM is as follows:

AAA-Registration Cancellation Acknowledgement	**<DIAMETER Header>**
	<Command-Code AVP = 338>
	<Destination-NAI AVP>
	<Host-Name AVP>
	<User-Name AVP>
	<Result-Code AVP>

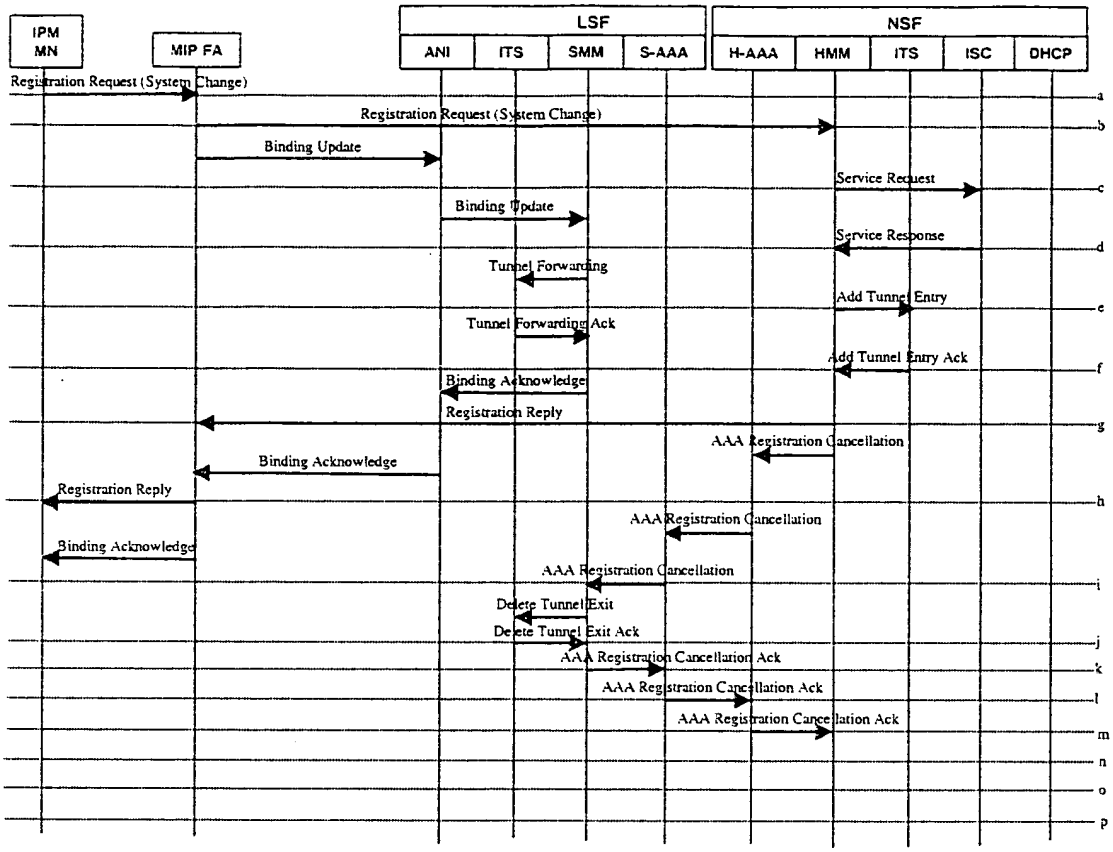
The AAA-Registration Cancellation Acknowledgement Message is of the format of DIAMETER. The SMM sends the message to the HMM with at least the mandatory fields. The Response-Code AVP indicates the failure or success of the AAA-Registration Cancellation Message.

The AVPs that can optionally be used in the AAA-Registration Cancellation Acknowledgement Message are,

- **Proxy-State AVP**
- **Time AVP**
- **Nonce AVP**
- **Integrity-Check-Value AVP**

and can be explained further in the AVPs Section 5.

3.5 IPM MN HANDOFFS FROM IPM ANI TO FA (SMOOTH HANDOFF)



IPM MN handoff from IPM ANI To FA (FA supports smooth handoff)

3.5.1 Registration Process

See Section 3.1.2

3.5.1.1 Registration Request and Message Format

See Section 3.1.2.1

3.5.1.2 Binding Update and Message Format

The Binding Update Message is used for notification of a mobile node's current mobility binding. It SHOULD be sent by the mobile node's home agent in response to a Binding Request Message, a Binding Warning Message, or the reception of a Binding Warning extension to a Registration Request. It SHOULD also be sent by a mobile node, or by the foreign agent with which the mobile node is registering, when notifying the mobile node's previous foreign agent that the mobile node has moved.

The **message format** exchanged between the MIP FA and the SMM is as follows:

Type	A	I	M	G	Rsvd	Lifetime
Mobile Node Home Address						
Care-of-Address						
Identification						
Extensions....						

- Type – 18.
- A – The 'A' (acknowledge) bit is set by the node sending the Binding Update Message to request a Binding Acknowledge Message be returned.
- I – The 'I' (identification present) bit is set by the node sending the Binding Update Message if the identification field is present in the message.
- M – If the 'M' (minimal encapsulation) bit is set, datagrams MAY be tunneled to the mobile node using the minimal encapsulation protocol.
- G – If the 'G' (Generic Record Encapsulation, or GRE) bit is set, datagrams MAY be tunneled to the mobile node using GRE.
- **Rsvd** – Reserved. Set as 0; ignored on reception.
- **Lifetime** – The number of seconds remaining before the binding cache entry must be considered expired. A value of all ones indicates infinity. A value of zero indicates that no binding cache entry for the mobile node should be created and that any existing binding cache entry (and visitor list entry, in the case of a mobile node's previous foreign agent) for the mobile node should be deleted. The lifetime is typically equal to the remaining lifetime of the mobile node's registration.
- **Mobile Node Home Address** – The home address of the mobile node to which the Binding Update Message refers.
- **Care-of-Address** – The current care-of-address of the mobile node. When set equal to the home address of the mobile node, the Binding Update Message instead indicates that no binding cache entry for the mobile node should be created, and any existing binding cache entry (and visitor list entry, in the case of a mobile node's previous foreign agent) for the mobile node should be deleted.
- **Identification** – If present, a 64-bit number, assigned by the node sending the Binding Request Message, is used to assist in matching requests with replies, and in protection against replay attacks.

3.5.1.3 Service Request and Message Format

See Section 3.1.2.2

3.5.1.4 Service Response and Message Format

See Section 3.1.2.3

3.5.1.5 Tunnel Forwarding and Message Format

The Tunnel Forwarding Message is sent by the SMM to instruct the ITS to set up a tunnel forwarding.

The **message format** exchanged between the SMM and the ITS is as follows:

Code (16)	Message Length (16)
Identification (64)	
Extensions...	

- **Code** – 5, For Tunnel Forwarding.
- **Message Length** – Length of the message including the header fields.
- **Identification** – Is used in matching requests and acknowledgements. The sender must ensure the identifier in a message is locally unique at any given time.

The Extensions used in the Tunnel Forwarding Message are,

- **Host NAI Extension**
- **Mobile Node IP Address Extension**
- **User NAI Extension (Optional)**
- **Lifetime Extension**
- **Tunnel Exit IP Address Extension**

and can be explained further in the Extension Section 4.

3.5.1.6 Add Tunnel Entry and Message Format

See Section 3.1.2.4

3.5.1.7 Tunnel Forwarding Acknowledgement and Message Format

The Tunnel Forwarding Acknowledgement Message is sent by the ITS to acknowledge the "Tunnel Forwarding" message. The identification field should be used for matching with the "Tunnel Forwarding" message.

The **message format** exchanged between the ITS and the SMM is as follows:

Code (16)	Message Length (16)
Identification (64)	
Extensions...	

- **Code** – 6, For Tunnel Forwarding Acknowledgement.
- **Message Length** – Length of the message including the header fields.
- **Identification** – Is used in matching requests and acknowledgements. The sender must ensure the identifier in a message is locally unique at any given time.

The Extensions used in the Tunnel Forwarding Acknowledgement Message are,

- **Host NAI Extension**
- **Mobile Node IP Address Extension**
- **User NAI Extension (Optional)**
- **Result Code Extension**

and can be explained further in the Extension Section 4.

3.5.1.8 Add Tunnel Entry Acknowledgement Format and Message Format

See Section 3.1.2.5

3.5.1.9 Binding Update Acknowledge and Message Format

The Binding Acknowledge Message is used to acknowledge receipt of a Binding Update Message, It SHOULD be sent by a node receiving a Binding Update Message if the acknowledge (A) bit is set in the Binding Update Message.

The **message format** exchanged between the SMM and the MN is as follows:

Type	Reserved	Status
Mobile Node Home Address		
Care-of-Address		
Identification		

- **Type** – 19.
- **Status** – If the Status is nonzero, this acknowledgement is negative. For instance, if the Binding Update was not accepted, but the incoming datagram has the Acknowledge flag set, then the status code should be set appropriately in the Binding Acknowledge Message.

- **Reserved**– Sent as 0; ignored on reception.

- **Mobile Node Home Address**– Copied from the Binding Update Message being acknowledged.
- **Identification** – Copied from the Binding Update Message being acknowledged, if present there.

3.5.1.10 Registration Reply and Message Format

See Section 3.1.2.6

3.5.1.11 AAA-Registration Cancellation and Message Format

See Section 3.4.1.7

3.5.1.12 Delete Tunnel Exit and Message Format

See Section 3.4.1.8

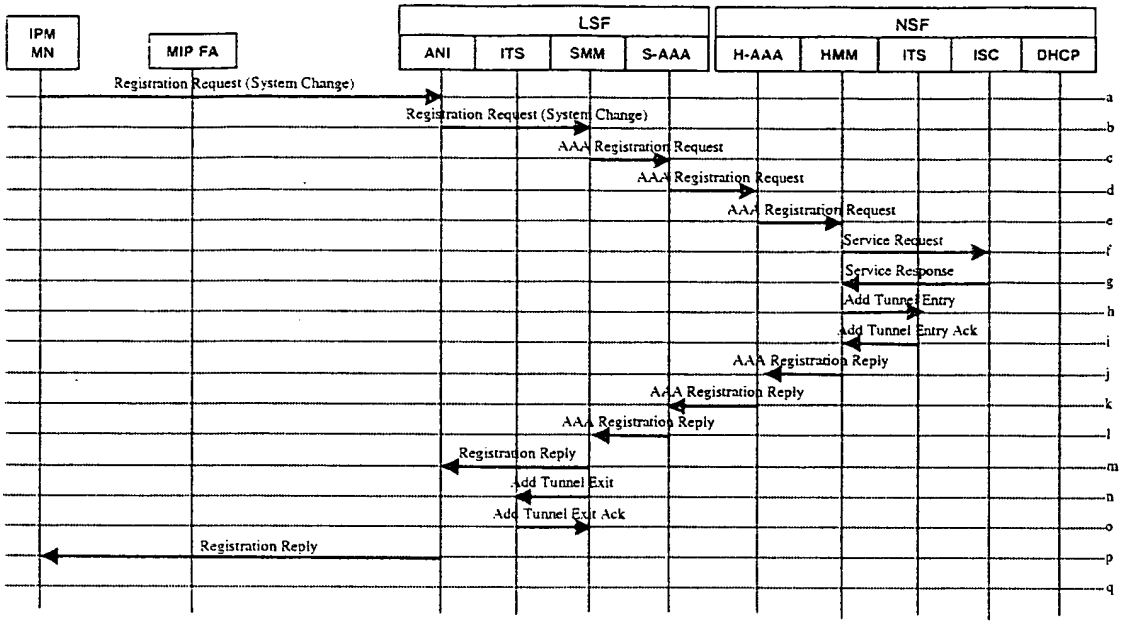
3.5.1.13 Delete Tunnel Exit Acknowledgement and Message Format

See Section 3.4.1.9

3.5.1.14 AAA-Registration Cancellation Acknowledgement and Message Format

See Section 3.4.1.10

3.6 IPM MN HANDOFFS FROM FA TO IPM ANI (NO SMOOTH HANDOFF)



IPM MN handoff from FA To IPM ANI (FA does not support smooth handoff)

3.6.1 Registration Process

See Section 3.1.2

3.6.1.1 Registration Request and Message Format

The Registration Request Message is sent by the IPM MN to the SMM to register for the service.

See Section 3.1.2.1 for the message format between the IPM MN and the SMM.

3.6.1.2 AAA-Registration Request and Message Format

The AAA-Registration-Request Message is used to carry out various kinds of registrations; these registrations are encapsulated in the IPM-Registration-Type AVP. This message is used by SMM to authenticate and authorize the user.

The message format exchanged between the SMM and the HMM is as follows:

AAA-Registration-Request	<DIAMETER Header>
	<Command-Code AVP = 335>
	<User-Name AVP>
	<Host-Name AVP>
	<IPM-Registration-Type AVP>
	<IPM-Registration-Request AVP>
	<IPM-Care-of-Address AVP>
	<IPM-Routing-Area-NAI AVP>

The AAA-Registration-Request Message is of the format of DIAMETER. The SMM sends the message to HMM with at least these mandatory fields. The IPM-Registration-Request AVP is the AVP which carries the message received from the MN, which is encapsulated in the AVP format for the Home domain to authenticate the user. The HMM processes this message based on the Registration-Type AVP, which carries the type of registration requested.

The AVPs that can optionally be used in the Registration Request Message are,

- **Destination-NAI AVP**
- **IPM-Client-Address AVP**
- **Home-Agent-Address AVP**
- **IPM-SMM-NAI AVP**
- **IPM-Terminal-Type AVP**
- **IPM-Profile-Type AVP**
- **Proxy-State AVP**
- **Timestamp AVP**
- **Nonce AVP/**
- **Integrity-Check-Value AVP**

and can be explained further in the AVP Section 5.

3.6.1.3 Service Request and Message Format

See Section 3.1.2.2

3.6.1.4 Service Response and Message Format

See Section 3.1.2.3

3.6.1.8 Registration Reply and Message Format

The Registration Reply Message is sent by the SMM to the IPM MN to indicate the result of the Registration Request Message sent.

See Section 3.1.2.6 for the message format exchanged between the SMM and the IPM MN.

3.6.1.9 Add Tunnel Exit and Message Format

The Add Tunnel Exit Message is sent by the SMM to instruct the ITS to set up a tunnel exit point.

The **message format** exchanged between the SMM and the ITS is as follows:

Code (16)	Message Length (16)
Identification (64)	
Extensions...	

- **Code** – 3, For Add Tunnel Exit.
- **Message Length** – Length of the message including the header fields.
- **Identification** – Is used in matching requests and acknowledgements. The sender must ensure the identifier in a message is locally unique at any given time.

The Extensions used in the Add Tunnel Exit Message are,

- **Host NAI Extension**
- **Lifetime Extension**
- **Mobile Node IP Address Extension**
- **User NAI Extension (Optional)**
- **Tunnel Exit IP Address Extension**

and can be explained further in the Extension Section 4.

3.6.1.10 Add Tunnel Exit Acknowledgement and Message Format

The Tunnel Exit Acknowledgement Message is sent by the ITS to acknowledge the "Add Tunnel Exit" Message.

The **message format** exchanged between the ITS and the SMM is as follows:

Code (16)	Message Length (16)
Identification (64)	
Extensions...	

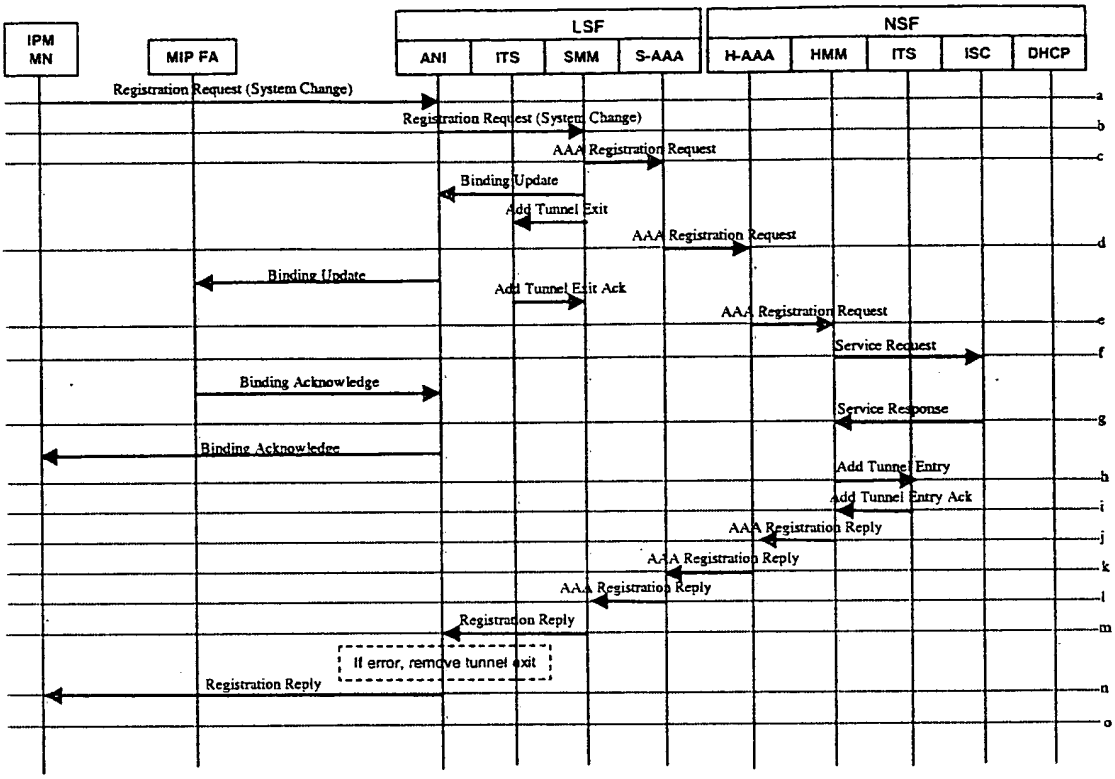
- **Code** – 4, For Add Tunnel Exit Acknowledgement Message.
- **Message Length** – Length of the message including the header fields.
- **Identification** – Is used in matching requests and acknowledgements. The sender must ensure the identifier in a message is locally unique at any given time.

The Extensions used in the Add Tunnel Exit Acknowledgement Message are,

- **Host NAI Extension**
- **Result Code Extension**
- **Mobile Node IP Address Extension (Optional)**
- **User NAI Extension (Optional)**
- **Tunnel Forwarding IP Address Extension**

and can be explained further in the Extension Section 4.

3.7 IPM MN HANDOFFS FROM FA TO IPM ANI (SMOOTH HANDOFF)



IPM MN handoff from FA To IPM ANI (FA supports smooth handoff)

3.7.1 Registration Process

See Section 3.1.2

3.7.1.1 Registration Request and Message Format

The Registration Request Message is sent by the IPM MN to the SMM to register for the service.

See Section 3.1.2.1 for the message format exchanged between the IPM MN and the SMM.

3.7.1.2 AAA-Registration Request and Message Format

See Section 3.6.1.2

3.7.1.3 Binding Update and Message Format

See Section 3.5.1.2

3.7.1.4 Add Tunnel Exit and Message Format

See Section 3.6.1.9

3.7.1.5 Add Tunnel Exit Acknowledgement and Message Format

See Section 3.6.1.10

3.7.1.6 Service Request and Message Format

See Section 3.1.2.2

3.7.1.7 Binding Acknowledge and Message Format

See Section 3.5.1.9

3.7.1.8 Service Response and Message Format

See Section 3.1.2.3

3.7.1.9 Add Tunnel Entry and Message Format

See Section 3.1.2.4

3.7.1.10 Add Tunnel Entry Acknowledgement and Message Format

See Section 3.1.2.5

3.7.1.11 AAA-Registration Reply and Message Format

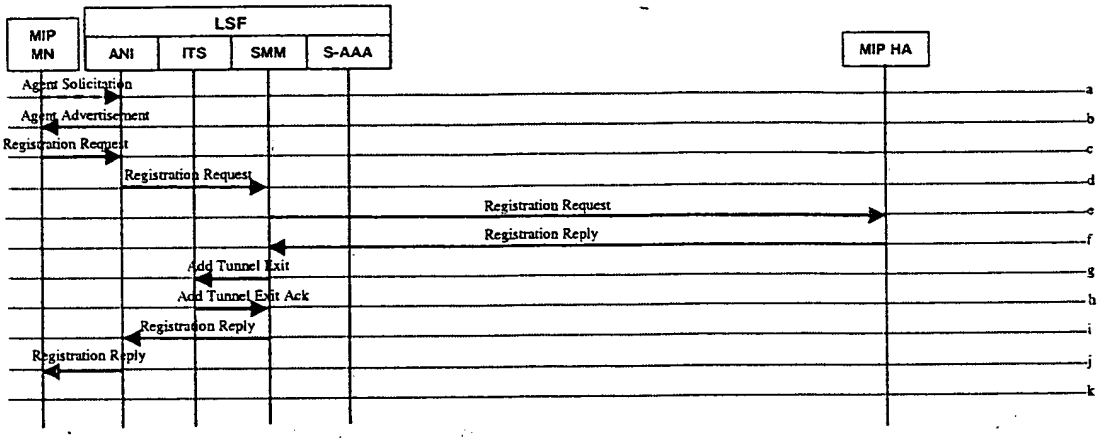
See Section 3.6.1.7

3.7.1.12 Registration Reply and Message Format

The Registration Reply Message is sent by the SMM to the IPM MN to indicate the result of the Registration Request Message sent.

See Section 3.1.2.6 for the message format exchanged between the SMM and the IPM MN.

3.8 MIP MN REGISTERS FROM MIP FA



MIP MN registers from IPM LSF

3.8.1 Agent Discovery Process

See Section 3.1.1

3.8.1.1 Agent Solicitation and Message Format

Agent Solicitation is the broadcast/multicast message sent by the MIP MN to detect a Service Provider in the event that the MIP MN has not received an Advertising Agent message.

See Section 3.1.1.1 for the message format exchanged between the MIP MN and the ANI.

3.8.1.2 Agent Advertisement and Message Format

Agent Advertisement are messages sent periodically, either as a broadcast or multicast for the visiting MIP MN to recognize the availability of service and to keep track of their point of attachment.

See Section 3.1.1.2 for the message format exchanged between the ANI and the MIP MN.

3.8.2 Registration Process

The purpose of registration is for the MIP MN to inform the MIP HA of its current location to which data packets can be forwarded to the MIP MN. The Registration process also includes the authenticating and authorizing of the MIP MN to have access to the visited network or LSF (Local Serving Function).

3.8.2.1 Registration Request and Message Format

The Registration Request Message is sent by the MIP MN to the MIP HA to register for the service.

See Section 3.1.2.1 for the message format exchanged between the MIP MN and the MIP HA.

3.8.2.2 Registration Reply and Message Format

The Registration Reply Message is sent by the MIP HA to the MIP MN to indicate the result of the Registration Request Message sent.

See Section 3.1.2.6 for the message format exchanged between the MIP HA and the MIP MN.

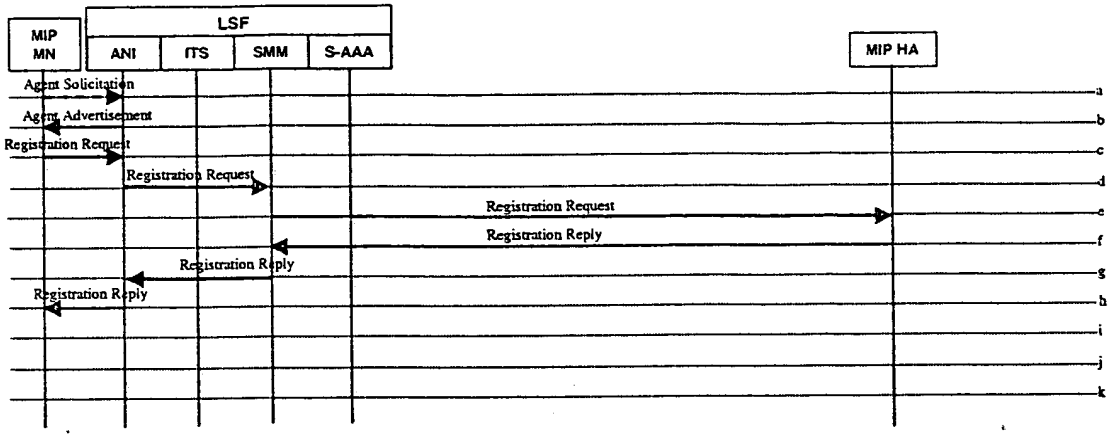
3.8.2.3 Add Tunnel Exit and Message Format

See Section 3.6.1.9

3.8.2.4 Add Tunnel Exit Acknowledgement and Message Format

See Section 3.6.1.10

3.9 MIP MN RE-REGISTERS FROM IPM LSF



MIP MN re-registers from IPM LSF

3.9.1 Agent Discovery Process

See Section 3.1.1

3.9.1.1 Agent Solicitation and Message Format

Agent Solicitation is the broadcast/multicast message sent by the MIP MN to detect a Service Provider in the event that the MIP MN has not received an Advertising Agent message.

See Section 3.1.1.1 for the message format exchanged between the MIP MN and the ANI.

3.9.1.2 Agent Advertisement and Message Format

Agent Advertisement are messages sent periodically, either as a broadcast or multicast for the visiting MIP MN to recognize the availability of service and to keep track of their point of attachment.

See Section 3.1.1.2 for the message format exchanged between the ANI and the MIP MN.

3.9.2 Registration Process

See Section 3.8.2

3.9.2.1 Registration Request and Message Format

The Registration Request Message is sent by the MIP MN to the MIP HA to register for the service.

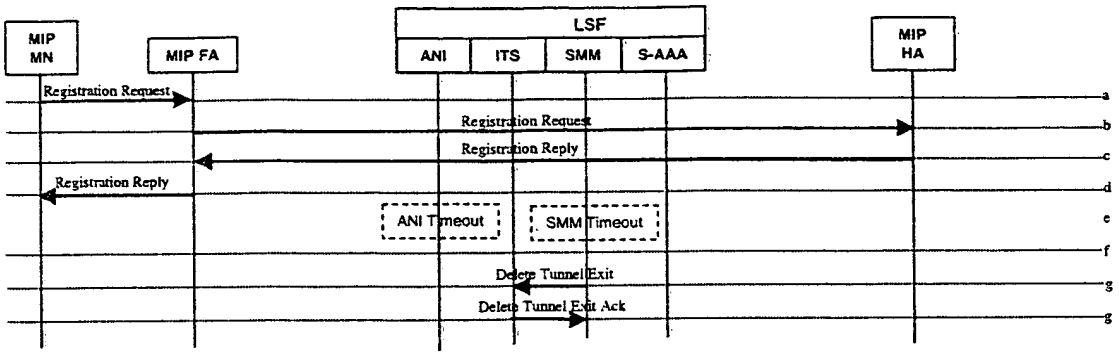
See Section 3.1.2.1 for the message format exchanged between the MIP MN and the MIP HA.

3.9.2.2 Registration Reply and Message Format

The Registration Reply Message is sent by the MIP HA to the MIP MN to indicate the result of the Registration Request Message sent.

See Section 3.1.2.6 for the message format exchanged between the MIP HA and the MIP MN.

3.10 MIP MN HANDOFFS FROM IPM ANI TO FA (NO SMOOTH HANDOFF)



MIP MN handoff from IPM ANI to FA(FA does not support smooth handoff)

3.10.1 Registration Process

See Section 3.8.2

3.10.1.1 Registration Request and Message Format

The Registration Request Message is sent by the MIP MN to the MIP HA to register for the service.

See Section 3.1.2.1 for the message format exchanged between the MIP MN and the MIP HA.

3.10.1.2 Registration Reply and Message Format

The Registration Reply Message is sent by the MIP HA to the MIP MN to indicate the result of the Registration Request Message sent.

See Section 3.1.2.6 for the message format exchanged between the MIP HA and the MIP MN.

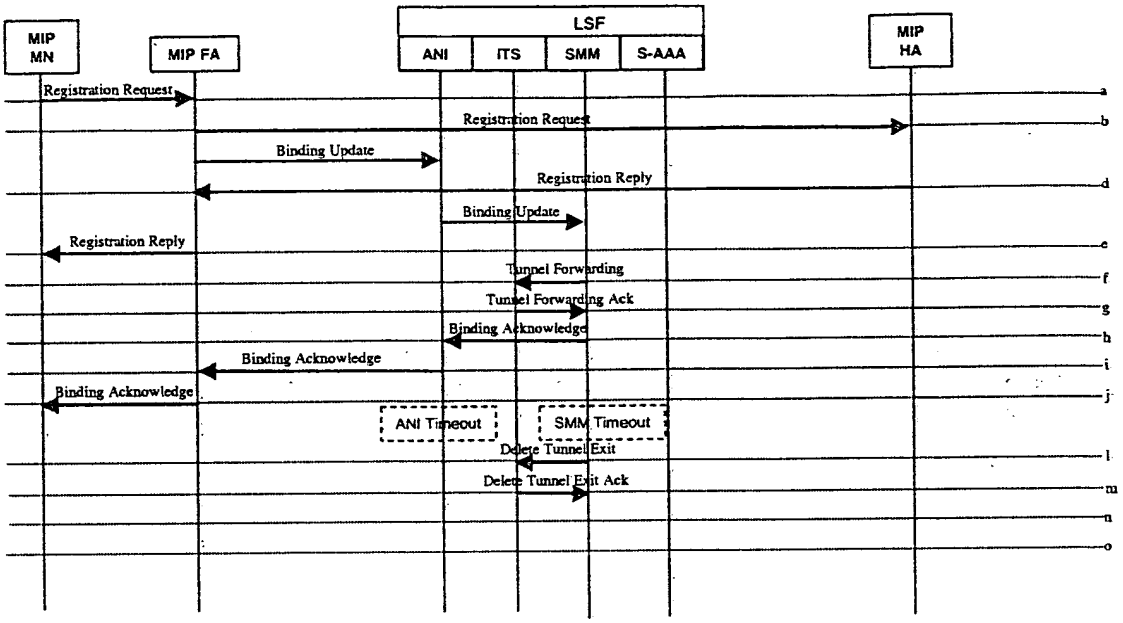
3.10.1.3 Delete Tunnel Exit and Message Format

See Section 3.4.1.8

3.10.1.4 Delete Tunnel Exit Acknowledgement and Message Format

See Section 3.4.1.9

3.11 MIP MN HANDOFFS FROM IPM ANI TO FA (SMOOTH HANDOFF)



MIP MN handoff from IPM ANI to FA(FA supports smooth handoff)

3.11.1 Registration Process

See Section 3.8.2

3.11.1.1 Registration Request and Message Format

The Registration Request Message is sent by the MIP MN to the MIP HA to register for the service.

See Section 3.1.2.1 for the message format exchanged between the MIP MN and the MIP HA.

3.11.1.2 Binding Update and Message Format

See Section 3.5.1.2

3.11.1.3 Registration Reply and Message Format

The Registration Reply Message is sent by the MIP HA to the MIP MN to indicate the result of the Registration Request Message sent.

See Section 3.1.2.6 for the message format exchanged between the MIP HA and the MIP MN.

3.11.1.4 Tunnel Forwarding and Message Format

See Section 3.5.1.5

3.11.1.5 Tunnel Forwarding Acknowledgement and Message Format

See Section 3.5.1.7

3.11.1.6 Binding Acknowledge and Message Format

See Section 3.5.1.9

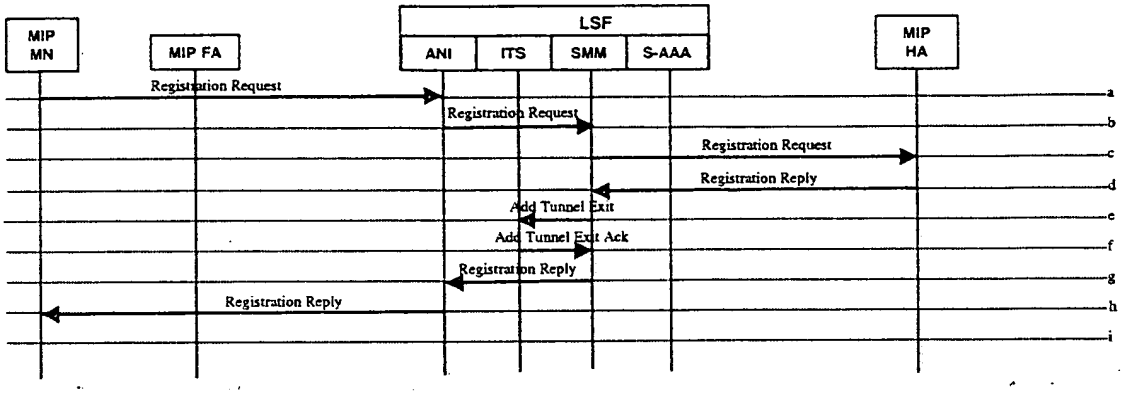
3.11.1.7 Delete Tunnel Exit and Message Format

See Section 3.4.1.8

3.11.1.8 Delete Tunnel Exit Acknowledgement and Message Format

See Section 3.4.1.9

3.12 MIP MN HANDOFFS FROM FA TO IPM ANI (NO SMOOTH HANDOFF)



MIP MN handoff from FA to IPM ANI (FA does not support smooth handoff)

3.12.1 Registration Process

See Section 3.8.2

3.12.1.1 Registration Request and Message Format

The Registration Request Message is sent by the MIP MN to the MIP HA to register for the service.

See Section 3.1.2.1 for the message format exchanged between the MIP MN and the MIP HA.

3.12.1.2 Registration Reply and Message Format

The Registration Reply Message is sent by the MIP HA to the MIP MN to indicate the result of the Registration Request Message sent.

See Section 3.1.2.6 for the message format exchanged between the MIP HA and MIP MN.

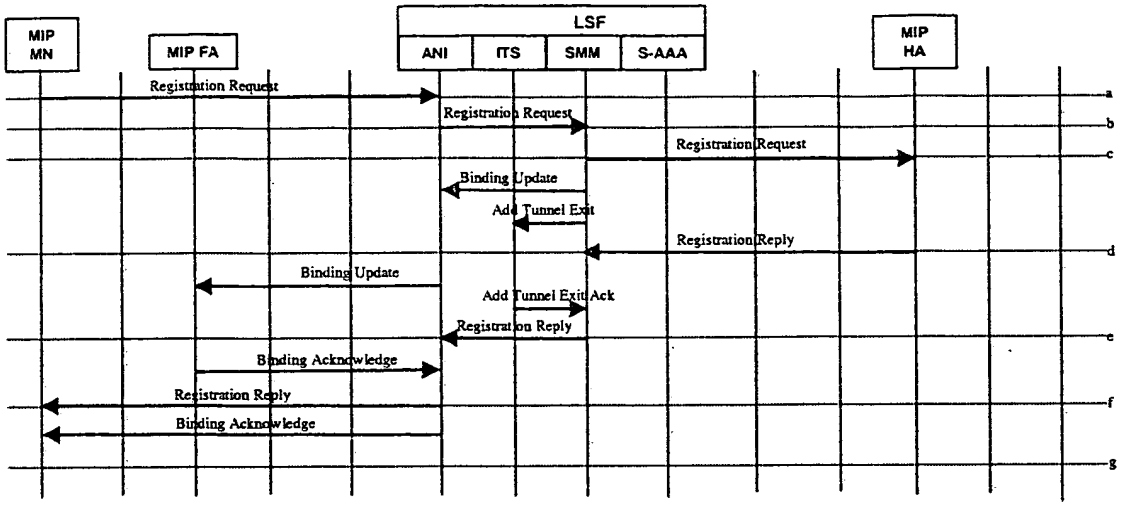
3.12.1.3 Add Tunnel Exit and Message Format

See Section 3.6.1.9

3.12.1.4 Add Tunnel Exit Acknowledgement and Message Format

See Section 3.6.1.10

3.13 MIP MN HANDOFFS FROM FA TO IPM ANI (SMOOTH HANDOFF)



MIP MN handoff from FA to IPM ANI (FA supports smooth handoff)

3.13.1 Registration Process

See Section 3.8.2

3.13.1.1 Registration Request and Message Format

The Registration Request Message is sent by the MIP MN to the MIP HA to register for the service.

See Section 3.1.2.1 for the message format exchanged between the MIP MN and the MIP HA.

3.13.1.2 Binding Update and Message Format

See Section 3.5.1.2

3.13.1.3 Add Tunnel Exit and Message Format

See Section 3.6.1.9

3.13.1.4 Registration Reply and Message Format

The Registration Reply Message is sent by the MIP HA to the MIP MN to indicate the result of the Registration Request Message sent.

See Section 3.1.2.6 for the message format exchanged between the MIP HA and the MIP MN.

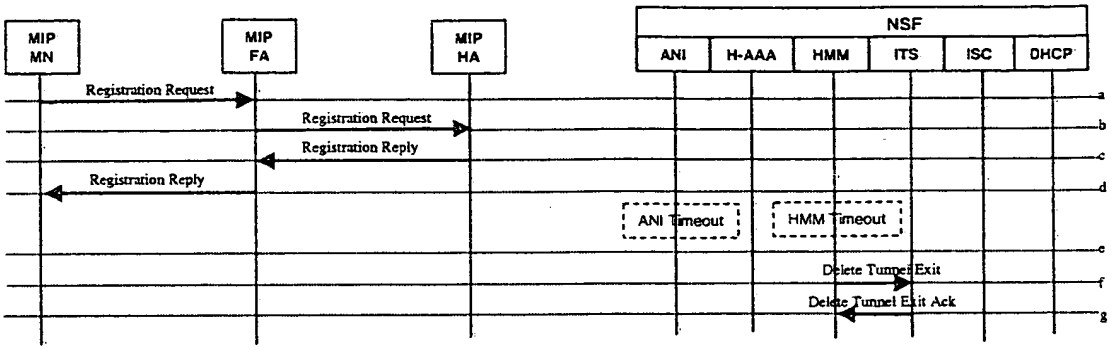
3.13.1.5 Add Tunnel Exit Acknowledgement and Message Format

See Section 3.6.1.10

3.13.1.6 Binding Acknowledge and Message Format

See Section 3.5.1.9

3.14 MIP MN HANDOFFS FROM NSF TO FA (NO SMOOTH HANDOFF)



MIP MN handoff from NSF to FA (FA does not support smooth handoff)

3.14.1 Registration Process

See Section 3.8.2

3.14.1.1 Registration Request and Message Format

The Registration Request Message is sent by the MIP MN to the MIP HA to register for the service.

See Section 3.1.2.1 for the message format exchanged between the MIP MN and the MIP HA.

3.14.1.2 Registration Reply and Message Format

The Registration Reply Message is sent by the MIP HA to the MIP MN to indicate the result of the Registration Request Message sent.

See Section 3.1.2.6 for the message format exchanged between the MIP HA and the MIP MN.

3.14.1.3 Delete Tunnel Exit and Message Format

The Delete Tunnel Exit Message is sent by the HMM to instruct the ITS to delete a tunnel exit point.

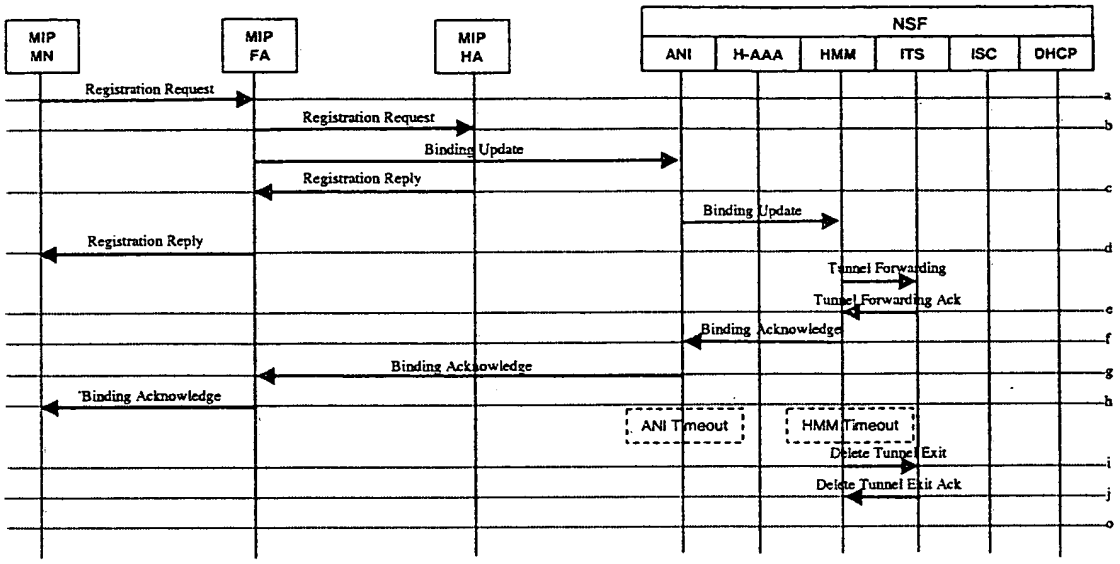
See Section 3.4.1.8 for the message format exchanged between the HMM and the ITS.

3.14.1.4 Delete Tunnel Exit Acknowledgement and Message Format

The Delete Tunnel Exit Acknowledgement Message is sent by the ITS to acknowledge the "Delete Tunnel Exit" Message. The identification field should be used for matching with the "Delete Tunnel Exit" Message.

See Section 3.4.1.9 for the message format exchanged between the ITS and the HMM.

3.15 MIP MN HANDOFFS FROM NSF TO FA (SMOOTH HANDOFF)



MIP MN handoff from NSF to FA (FA supports smooth handoff)

3.15.1 Registration Process

See Section 3.8.2

3.15.1.1 Registration Request and Message Format

The Registration Request Message is sent by the MIP MN to the MIP HA to register for the service.

See Section 3.1.2.1 for the message format exchanged between the MIP MN and the MIP HA.

3.15.1.2 Binding Update and Message Format

See Section 3.5.1.2

3.15.1.3 Registration Reply and Message Format

The Registration Reply Message is sent by the MIP HA to the MIP MN to indicate the result of the Registration Request Message sent.

See Section 3.1.2.6 for the message flow exchanged between the MIP HA and the MIP MN.

3.15.1.4 Tunnel Forwarding and Message Format

The Tunnel Forwarding Message is sent by the HMM to instruct the ITS to set up a tunnel forwarding.

See Section 3.5.1.5 for the message format exchanged between the HMM and the ITS.

3.15.1.5 Tunnel Forwarding Acknowledgement and Message Format

The Tunnel Forwarding Acknowledgement Message is sent by the ITS to acknowledge the "Tunnel Forwarding" message. The identification field should be used for matching with the "Tunnel Forwarding" message.

See Section 3.5.1.7 for the message format exchanged between the ITS and the HMM.

3.15.1.6 Binding Acknowledge and Message Format

See Section 3.5.1.9

3.15.1.7 Delete Tunnel Exit and Message Format

The Delete Tunnel Exit Message is sent by the HMM to instruct the ITS to delete a tunnel exit point.

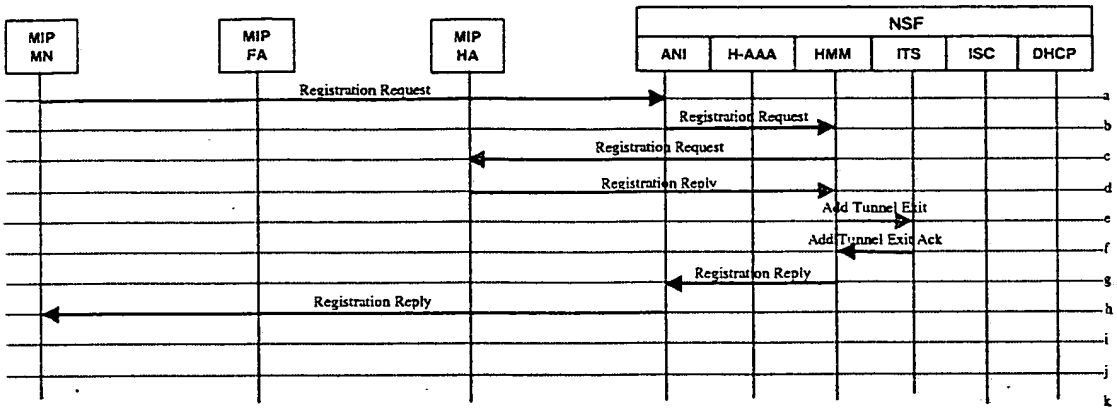
See Section 3.4.1.8 for the message format exchanged between the HMM and the ITS.

3.15.1.8 Delete Tunnel Exit Acknowledgement and Message Format

The Delete Tunnel Exit Acknowledgement Message is sent by the ITS to acknowledge the "Delete Tunnel Exit" Message. The identification field should be used for matching with the "Delete Tunnel Exit" Message.

See Section 3.4.1.9 for the message format exchanged between the ITS and the HMM.

3.16 MIP MN HANDOFFS FROM FA TO NSF (NO SMOOTH HANDOFF)



MIP MN handoff from FA to NSF (FA does not support smooth handoff)

3.16.1 Registration Process

See Section 3.8.2

3.16.1.1 Registration Request and Message Format

The Registration Request Message is sent by the MIP MN to the MIP HA to register for the service.

See Section 3.1.2.1 for the message format exchanged between the MIP MN and the MIP HA.

3.16.1.2 Registration Reply and Message Format

The Registration Reply Message is sent by the MIP HA to the MIP MN to indicate the result of the Registration Request Message sent.

See Section 3.1.2.6 for the message format exchanged between the MIP HA and MIP MN.

3.16.1.3 Add Tunnel Exit and Message Format

The Add Tunnel Exit Message is sent by the HMM to instruct the ITS to set up a tunnel exit point.

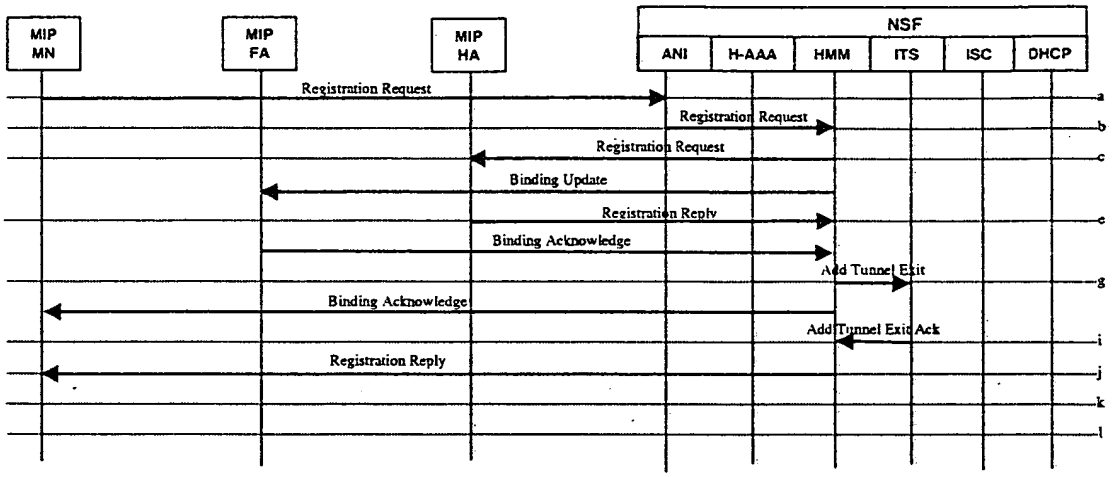
See Section 3.6.1.9 for the message format exchanged between the HMM and the ITS.

3.16.1.4 Add Tunnel Exit Acknowledgement and Message Format

The Tunnel Exit Acknowledgement Message is sent by the ITS to acknowledge the "Add Tunnel Exit" Message.

See Section 3.6.1.10 for the message format exchanged between the ITS and the HMM.

3.17 MIP MN HANDOFFS FROM FA TO NSF (NO SMOOTH HANDOFF)



MIP MN handoff from FA to NSF (FA supports smooth handoff)

3.17.1 Registration Process

See Section 3.8.2

3.17.1.1 Registration Request and Message Format

The Registration Request Message is sent by the MIP MN to the MIP HA to register for service.

See Section 3.1.2.1 for the message format exchanged between the MIP MN and the MIP HA.

3.17.1.2 Binding Update and Message Format

See Section 3.5.1.2

3.17.1.3 Registration Reply and Message Format

The Registration Reply Message is sent by the MIP HA to the MIP MN to indicate the result of the Registration Request Message sent.

See Section 3.1.2.6 for the message format exchanged between the MIP HA and the MIP MN.

3.17.1.4 Binding Acknowledge and Message Format

See Section 3.5.1.9

3.17.1.5 Add Tunnel Exit and Message Format

The Add Tunnel Exit Message is sent by the HMM to instruct the ITS to set up a tunnel exit point.

See Section 3.6.1.9 for the message format exchanged between the HMM and the ITS.

3.17.1.6 Add Tunnel Exit Acknowledgement and Message Format

The Tunnel Exit Acknowledgement Message is sent by the ITS to acknowledge the "Add Tunnel Exit" Message.

See Section 3.6.1.10 for the message format exchanged between the ITS and the HMM.

4. EXTENSIONS

4.1 AGENT DISCOVERY EXTENSIONS

4.1.1 ANI-NAI Extension

The ANI-NAI Extension is used to carry the ANI information, such as ANI's NAI (Network Access Identifier).

Type (8)	Length (8)	Sub-Type (8)	Rsvd (8)
ANI-NAI...			

- **Type** – IPM-VENDOR-SPECIFIC-EXTENSION (255).
- **Length** – Length of the ANI-NAI string + 2 bytes.
- **Sub-Type** – The sub-type of extension (1).
- **Rsvd** – Reserved byte.
- **ANI-NAI** – The NAI string of the ANI.

4.1.2 Mobility Agent Advertisement Extension

The Mobility Agent Advertisement Extension is added to the ICMP Router Advertisement message to indicate to MNs that this is an Agent Advertisement message (not an Router Advertisement message) with the specified Care-of Addresses.

Type	Length	Sequence Number							
Registration Lifetime		R	B	H	F	M	G	V	Reserved
Zero or more Care-of-Address(es)									

- **Type** – 16
- **Length** – (6 + 4*N), where N is the number of Care-of-Address(es) advertised.
- **Sequence Number** – The count of Agent Advertisement Messages sent since the agent was initialized.
- **Registration Lifetime** – The longest lifetime (measured in seconds) that this agent is willing to accept in any Registration Request Message. A value of 0xffff indicates infinity. This field has no relation to the "lifetime" field within the ICMP router advertisement portion of the Agent Advertisement Message.
- **R** – Registration required. Registration with this foreign agent (or another foreign agent on this link) is required rather than using a co-located Care-of-Address.
- **B** – Busy. The foreign agent will not accept registrations from additional mobile nodes.

- **H** – Home agent. This agent offers service as a home agent on the link on which this Agent Advertisement Message is sent.
- **F** – Foreign agent. This agent offers service as a foreign agent on the link on which this Agent Advertisement Message is sent.
- **M** – Minimal encapsulation. This agent implements receiving tunneled datagrams that use minimal encapsulation [15].
- **G** – GRE encapsulation. This agent implements receiving tunneled datagrams that use GRE encapsulation [8].
- **V** - Van Jacobson header compression. This agent support use of Van Jacobson header compression [10] over the link with any registered mobile node.
- **Reserved** – Sent as zero; ignored on reception.
- **Care-of-Address(es)** – The advertised foreign agent Care-of-Addres(es) provided by this foreign agent. An Agent Advertisement Message MUST include at least one Care-of Address if the 'F' bit is set. The length field in the extension determines the number of Care-of-Address(es) present.

4.1.3 One-byte Padding Extension

Some IP protocol implementations insist upon padding ICMP messages to an even number of bytes. If the ICMP length of an Agent Advertisement is odd, this extension MAY be included in order to make the ICMP length even. This extension is NOT intended to be a general purpose extension to be included in order to word or long align the various fields of the Agent Advertisement. An Agent Advertisement SHOULD NOT include more than one One-byte Padding Extension, and if present, this extension SHOULD be the last extension in the Agent Advertisement.

Note that unlike other extensions used in Mobile IP, the One-byte Padding Extension is encoded as a single byte, with no "Length" not "Data" field present.

Type

Type – 0 (One-byte Padding Extension)

4.1.4 Prefix-Lengths Extension

The Prefix-Lengths Extension MAY follow the Mobility Agent Advertisement Extension. It is used to indicate the number of bits of network prefix that applies to each Router Address listed in the ICMP Router Advertisement portion of the Agent Advertisement. Note that the prefix lengths given DO NOT apply to care-of address(es) listed in the Mobility Agent Advertisement Extension.

Type	Length	Prefix Length	....

- **Type** – 19 (Prefix-Lengths Extension)

- **Length** – N, where N is the value (possibly zero) of the NUM Addrs field in the ICMP Router Advertisement portion of the Agent Advertisement.
- **Prefix Length(s)** – The number of leading bits that define the network number of the corresponding Router Address listed in the ICMP Router Advertisement portion of the message. The prefix length for each Router Address is encoded as a separate byte, in the order that the Router Addresses are listed in the ICMP Router Advertisement portion of the message.

4.2 ITS CONTROL EXTENSIONS

All of the extensions for ITS Messages have the following format:

Code (16)	Extension Length (16)
Data....	

- **Code** – Defined.
- **Extension Length** – Length of the extension including header fields.
- **Data** – Variable depending upon the extension type.

4.2.1 Authentication Extension

The Authentication Extension is used by the ITS to authenticate the requesting message before performing the requested action.

- **Code** – 10 for Authentication Extension type.
- **Extention Length** – TBD
- **Data** – TBD

4.2.2 Flag Extension

The Flag Extension is used only if the message type is "Add Tunnel Entry". If this Extension is missing, the application should assume that all flags are zero.

- **Code** – 3 for Flag Extension type.
- **Extension Length** – Length is 6 bytes.
- **Data** – Is a 16-bit value with the lower byte contains the flags as defined in RFC 2002 for Registration Request Message.

4.2.3 Host NAI Extension

The Host NAI Extension is used to let the IPM Tunnel Service (ITS) server to know which node a request message comes from. The ITS can maintain the request information per each requesting node so that it can clean up resources for that requesting node when necessary. (Ex. Requesting node is down abnormally).

- **Code** – 1 for Host NAI Extension type.
- **Extension Length** – Variable.
- **Data** – Contains a Host NAI string.

4.2.4 Lifetime Extension

The Lifetime Extension is required for "Add Tunnel Entry", "Add Tunnel Exit", and "Tunnel Forwarding". It is required for ITS to implement the session timeout.

- **Code** – 4 for Lifetime Extension type.
- **Extension Length** – Length is 8 bytes.
- **Data** – Is a 32-bit value.

4.2.5 Mobile Node IP Address Extension

The Mobile Node IP Address Extension is required for all messages except "Delete all..." messages.

- **Code** – 5 for Mobile Node IP Address Extension type.
- **Extension Length** – 8 bytes for Ipv4 and 20 bytes for Ipv6.
- **Data** – Contains the IP address of the Mobile Node.

4.2.6 Result Code Extension

The Result Code Extension is required for all acknowledgement messages.

- **Code** – 9 for Result Code Extension type.
- **Extension Length** – 6 bytes.
- **Data** – Contains the result code of the previous request message.
  - 0 = No error.
  - 1 = TBD, etc.

4.2.7 Tunnel Entry IP Address Extension

The Tunnel Entry IP Address Extension is required only for "Add Tunnel Entry" and "Delete Tunnel Entry".

- **Code** – 6 for Tunnel Entry IP Address Extension type.
- **Extension Length** – 8 bytes for Ipv4 and 20 bytes for Ipv6.
- **Data** – Contains the IP address of the Tunnel Entry IP Address.

4.2.8 Tunnel Exit IP Address Extension

The Tunnel Exit IP Address Extension is required only for "Add Tunnel Exit", "Tunnel Forwarding", and "Delete Tunnel Exit".

- **Code** – 7 for Tunnel Exit IP Address Extension type.
- **Extension Length** – 8 bytes for Ipv4 and 20 bytes for Ipv6.
- **Data** – Contains the IP address of the Tunnel Exit IP Address.

4.2.9 Tunnel Forwarding IP Address Extension

The Tunnel Forwarding IP Address Extension is only required for "Tunnel Forwarding".

- **Code** – 8 for Tunnel Forwarding IP Address Extension type.
- **Extension Length** – 8 bytes for Ipv4 and 20 bytes for Ipv6.
- **Data** – Contains the IP Address of the Tunnel Forwarding IP Address.

4.2.10 User-NAI Extension

The User-NAI Extension contains the User NAI string.

- **Code** – 2 for User NAI Extension type.
- **Extension Length** – Variable.
- **Data** – The User-NAI string.

4.3 IPM REGISTRATION EXTENSIONS

4.3.1 ANI-HMM Authentication Extension

The ANI-HMM Authentication Extension is used in the Registration Messages to carry the Authentication Extension between ANI and HMM.

Type (8)	Length (8)	Sub-Type (8)	Rsvd (8)
Authenticator (32)			

- **Type** – IPM_VENDOR_SPECIFIC_EXTENSION (255)
- **Length** – Length of Authenticator + 2 bytes.
- **Sub-Type** – Sub-type of the extension (6).
- **Rsvd** – Reserved byte.
- **Authenticator** – The authenticator calculated over the entire message up to the extension header.

4.3.2 ANI-SMM Authentication Extension

The ANI-SMM Authentication Extension is used in the Registration Messages to carry the Authentication Extension between ANI and SMM.

Type (8)	Length (8)	Sub-Type (8)	Rsvd (8)
Authenticator			

- **Type** – IPM-VENDOR-SPECIFIC-EXTENSION (255).
- **Length** – Length of authenticator + 2 bytes.
- **Sub-Type** – The sub-type of extension (5).
- **Rsvd** – Reserved byte.
- **Authenticator** – The authenticator calculated over the entire message up to the extension header.

4.3.3 L2-Address Extension

The L2-Address Extension is used in the Registration Request Message to carry the MN's L2 Address.

Type (8)	Length (8)	Sub-Type (8)	Address Type (8)
Address			

- **Type** – IPM-VENDOR-SPECIFIC-EXTENSION (255).
- **Length** – Length of the address + 2 bytes.
- **Sub-Type** – The sub-type of extension (9).
- **Address Type** – The Address-Type of the Mobile Node. The current address types are:
  - 802.3 Address
  - 802.11 Address
  - IMSI
  - MIN
- **Address** – Layer 2 address of the Mobile Node.

4.3.4 Local Registration Lifetime Extension

The Local Registration Lifetime Extension is used to carry the lifetime of local registration.

Type (8)	Length (8)	Sub-Type (8)	Rsvd (8)
Lifetime (32)			

- **Type** – IMP_VENDOR_SPECIFIC_EXTENSION (255)
- **Length** – 6 bytes.
- **Sub-Type** – The sub-type of the extension (10).
- **Rsvd** – Reserved byte.
- **Lifetime** – The lifetime allowed by SMM for local re-registration in seconds.

4.3.5 MN-Home Authentication Extension

The MN-Home Authentication Extension is used in the Registration Messages to carry the Authentication Extension between the MN and Home.

Type (8)	Length (8)	Sub-Type (8)	Rsvd (8)
Authenticator			

- **Type** – IPM-VENDOR-SPECIFIC-EXTENSION (255).
- **Length** – Length of authenticator + 2 bytes.
- **Sub-Type** – The sub-type of extension (3).
- **Rsvd** – Reserved byte.
- **Authenticator** – The authenticator calculated over the entire message up to the extension header.

4.3.6 MN-SMM Authentication Extension

The MN-SMM Authentication Extension is used in the Registration Message to carry the Authentication Extension between MN and SMM.

Type (8)	Length (8)	Sub-Type (8)	Rsvd (8)
Authenticator			

- **Type** – IPM-VENDOR-SPECIFIC-EXTENSION (255).
- **Length** – Length of Authenticator + 2 bytes.
- **Sub-Type** – The sub-type of extension (4).
- **Rsvd** – Reserved byte.
- **Authenticator** – The authenticator calculated over the entire message up to the extension header.

4.3.7 Foreign-Home Authentication Extension

The Foreign-Home Authentication Extension MAY be included in Registration Requests and Replies in cases in which a mobility security association exists between the foreign agent and the home agent.

Type	Length	SPI ....
... SPI (cont.)		Authenticator ...

- **Type** – 34.
- **Length** – 4 plus the number of bytes in the Authenticator.
- **SPI** – Security Parameter Index (4 bytes). An opaque identifier.
- **Authenticator** – Variable length.

4.3.8 Mobile-Foreign Authentication Extension

The Mobile-Foreign Authentication Extension MAY be included in Registration Requests and Replies in cases in which a mobility security association exists between the mobile node and the foreign agent.

Type	Length	SPI ....
... SPI (cont.)		Authenticator ...

- **Type** – 33.
- **Length** – 4 plus the number of bytes in the Authenticator.
- **SPI** – Security Parameter Index (4 bytes). An opaque identifier.
- **Authenticator** – Variable length.

4.3.9 Mobile-Home Authentication Extension

Exactly one Mobile-Home Authentication Extension MUST be present in all Registration Requests and Registration Replies, and is intended to eliminate problems, which can result from the uncontrolled propagation of remote redirects in the Internet. The location of the extension marks the end of the authenticated data.

Type	Length	SPI ....
... SPI (cont.)		Authenticator ...

- **Type** – 32.
- **Length** – 4 plus the number of bytes in the Authenticator.
- **SPI** – Security Parameter Index (4 bytes). An opaque identifier.
- **Authenticator** – Variable length.

4.3.10 Previous-SMM-NAI Extension

The Previous-SMM-NAI Extension is used in the Registration Request Message to carry the previous SMM's NAI. This Extension is not applicable with Registration type of "Initial Registration".

Type (8)	Length (8)	Sub-Type (8)	Rsvd (8)
SMM-NAI...			

- **Type** – IPM-VENDOR-SPECIFIC-EXTENSION (255).
- **Length** – Length of the SMM-NAI string + 2 bytes.
- **Sub-Type** – The sub-type of extension (8).
- **Rsvd** – Reserved byte.
- **SMM-NAI** – The NAI string of the SMM.

4.3.11 Registration-Type Extension

The Registration-Type Extension is used in the Registration Request Message to indicate what type of registration is requested.

Type (8)	Length (8)	Sub-Type (8)	Rsvd (8)
Registration-Type (32)			

- **Type** – IPM-VENDOR-SPECIFIC-EXTENSION (255).
- **Length** – Length is 6 bytes.
- **Sub-Type** – The sub-type of extension (2).
- **Rsvd** – Reserved byte.
- **Registration-Type** – Registration types.

Currently, the types of Registration are:

- Initial Registration (0)
- De-Registration (1)
- System-Change (2)
- ANI-Change (3)
- Local Re-Registration (4)
- Re-Registration (5)
- Clean-up (6)

4.3.12 SMM Key Extension

The SMM Key Extension is used to carry the shared secret key that is to be used between the SMM and MN.

Type (8)	Length (8)	Sub-Type (8)	Rsvd (8)
SMM-Key			

- **Type** – IMP_VENDOR_SPECIFIC_EXTENSION (255)
- **Length** – Length of the SMM Key + 2 bytes.
- **Sub-Type** – The sub-type of the extension (7).
- **Rsvd** – Reserved byte.
- **SMM Key** – The SMM Key, which is encrypted using the MN-Home shared secret key.

4.3.13 SMM-NAI Extension

The SMM-NAI Extension carries the SMM-NAI in the IPM messages.

Type (8)	Length (8)	Sub-Type (8)	Rsvd (8)
SMM-NAI...			

- **Type** – IMP_VENDOR_SPECIFIC_EXTENSION (255)
- **Length** – Length of the SMM-NAI string + 2 bytes.
- **Sub-Type** – The sub-type of the extension (0).
- **Rsvd** – Reserved byte.
- **SMM-NAI** – The NAI string of the SMM.

4.3.14 User-NAI Extension

The User-NAI Extension contains the User NAI string.

Type (8)	Length (8)	User-NAI...

- Type – Extension (131).
- Length – Length of User-NAI.
- User-NAI – The User-NAI string.

4.4 IPM SECURITY EXTENSIONS

4.4.1 Control Message Authentication Request Extension

The Control Message Authentication Request Extension is used when

Type	Sub-Type	Payload Length
Attribute Values.....		

- **Type** – IPM_EXT.
- **Sub-Type**:
  - CNTL_MSG_AUTH_EXT.
- **Payload Length** – Length of all the attributes values.
- **Attribute Values**:

The Attributes used in the Control Message Authentication Extension are,

- **Data Authentication Request Attribute**

depending upon these variables:

- When the Sub-Type is 0, there is no Attribute.
- When the Sub-Type is 1, the Data Authentication Request Attribute applies.
- When the Sub-Type is 2, the Data Authentication Reply Attribute applies.

and can be explained further in the Attribute Section 6.

4.4.2 Control Message Authentication Reply Extension

The Control Message Authentication Reply Extension is used when

Type	Sub-Type	Payload Length
Attribute Values.....		

- **Type** – IPM_EXT..
- **Sub-Type**:
  - CNTRL_MSG_AUTH_EXT.
- **Payload Length** – Length of all the attributes values.
- **Attribute Values**:

The Attributes used in the Control Message Authentication Extension are,

- **Data Authentication Reply Attribute**

depending upon these variables:

- When the Sub-Type is 0, there is no Attribute.
- When the Sub-Type is 1, the Data Authentication Request Attribute applies.
- When the Sub-Type is 2, the Data Authentication Reply Attribute applies.

and can be explained further in the Attribute Section 6.

4.4.3 Session Key Allocation Extension

The Session Key Allocation Extension is used when allocation of a secret or a public session key is required. The sub-type field value of this extension determines if it is used in the Request Message or Reply Message.

Type	Sub-Type	Payload Length
Attribute Values.....		

- **Type** – KEY_ALLOCATION_ EXT.
- **Sub-Type**:
  - 1 (Session Key Allocation Request Extension)
  - 2 (Session Key Allocation Reply Extension, single key allocated)

- 3 (Session Key Allocation Reply Extension, duplicate key allocated)

- **Payload Length** – Length of all the attributes values.
- **Attribute Values**:

The Attributes used in the Session Key Allocation Extension are,

- **Secret Key Request Data Attribute**
- **Single Secret Key Reply Data Attribute**
- **Duplicate Secret Key Reply Data Attribute**

depending upon these variables:

- When the Sub-Type is 1, the Secret Key Request Data Attribute applies.
- When the Sub-Type is 2, the Single Secret Key Reply Data Attribute applies.

- When the Sub-Type is 3, the Duplicate Secret Key Reply Data Attribute applies.

and can be explained further in the Attribute Section 6.

4.4.4 Session Key Delete Extension

The Session Key Delete Extension is used when the delete of a secret or public session key is required.

Type	Sub-Type	Payload Length
Key ID 0		
.		
.		
Key ID N		

- **Type** – IPM_EXTENSIONS.
- **Sub-Type** – SESSION_KEY_DELETE_REQUEST_EXT.
- **Payload Length** – 4 + 4 * Number of Keys (octets).
- **Key ID** – The Key ID assigned by the User Authentication Server.

4.4.5 Session Key Lifetime Renewal Extension

The Session Key Lifetime Renewal Extension is used when the renewal of a secret or public session key lifetime is required. Also, it is added to the User Service Reply message if the request is honored by the User Authentication Server.

Type	Sub-Type	Payload Length
Lifetime 0		
Key ID 0		

Lifetime N
Key ID N

- **Type** – IPM_EXTENSIONS.
- **Sub-Type** – SESSION_KEY_LIFETIME_RENEWAL_EXT.
- **Payload Length** – 4 + 8 * Number of Keys (octets).
- **Lifetime** – Required new lifetime for the key.
- **Key ID** – It is the ID for the key to extend his lifetime.

4.4.6 User Authentication Information Extension

The User Authentication Information Extension can only be sent in the User Service Request Message. It contains all the needed data attributes, which contain the required information about the user for the process of verification and authentication (e.g. SSN, Account Number, etc.).

Type	Sub-Type	Payload Length
Data Attributes		

- **Type** – USER_AUTH_INFO_EXT.
- **Sub-Type** – 0.
- **Payload Length** – Length of all the attributes values.

The Attributes used in the User Authentication Information Extension are,

- **Account Number Data Attribute**
- **SSN Data Attribute (Optional)**
- **User Name Data Attribute (Recommended)**
- **User Birthday Data Attribute (Recommended)**
- **User Password Data Attribute (Optional)**
- **User Address Data Attribute (Optional)**
- **User Home Phone Number Data Attribute (Optional)**
- **User Work Phone Number Data Attribute (Optional)**
- **User NAI Data Attribute (Recommended)**
- **User PIN Number Data Attribute (Optional)**
- **Digital Signature Data Attribute (Recommended)**

and can be explained further in the Attribute Section 6.

5. AVPS

AVPs is a method of encapsulating information relevant to the DIAMETER message.

DIAMETER AVPs carry specific authentication, accounting and authorization information, security information as well as configuration details for the request and reply messages.

The AVP format is shown below and MUST be sent in network byte order.

AVP Code						
AVP Length	Reserved	P	T	V	R	M
Vendor ID (Optional)						
Tag (Optional)						
Data...(depends on the particular AVP)						

- **AVP Code** – The AVP Code identifies the attribute uniquely.
- **AVP Length** – The AVP Length field is two octets, and indicates the length of this attribute including the AVP Code, AVP Length, AVP Flags, Reserved, The Tag and Vendor ID fields if present and the AVP data.
- **AVP Flags** – The AVP Flags field informs the DIAMETER host how each attribute must be handled.

  - **"R" bit and Reserved Bit** – Are used and should be set to 0 and ignored on receipt, while the "P" bit is defined.
  - **"M" bit** – Known as the mandatory bit, indicates whether support of the AVP is required.
  - **"V" bit** – Known as the Vendor-Specific bit, indicates whether the optional Vendor ID field is present in the AVP header.
  - **"T" bit** – Known as the Tag bit, is used to group sets of AVPs together. Grouping AVPs is necessary when more than one AVP is needed to express a condition.

- **Vendor ID** – The Vendor ID field is present in the "V" bit and is set in the AVP Flags field.
- **Tag** – The Tag field is four octet in length and is intended to provide a means of grouping attributes in the same message which refer to the same set. If the Tag field is unused, the "T" bit MUST NOT be set.
- **Data** – The Data field is zero or more octets and contains information specific to the attribute. The format and length of the Data field is determined by the AVP Code and AVP Length fields. The format of the value field MAY be one of seven data types.

- **Data** – The data contains a variable length of arbitrary data. Unless otherwise noted, the AVP Length field MUST be set to at least 9.
- **String** – The data contains a non-NULL terminated variable length string using the UTF-8 [24] character set. Unless otherwise noted, the AVP Length field MUST be set to at least 9.
- **Address** – 32 bit (Ipv4) [17] or 128 bit (Ipv6) [16] address, most significant octet first. The format of the address (Ipv4 or Ipv6) is determined by the length. If the attribute value is an Ipv4 address, the AVP Length field MUST be 12, otherwise the AVP Length field MUST be set to 24 for Ipv6 addresses.
- **Integer32** – 32-bit value, in network byte order. The AVP Length field MUST be set to 12.
- **Integer64** - 64-bit value, in network byte order. The AVP Length field MUST be set to 16.
- **Time** – 32-bit unsigned value, in network byte order, and contains the seconds since 00:00:00 GMT, January 1, 1900. The AVP Length field MUST be set to 12.
- **Complex** – The complex data type is reserved for AVPs that includes multiple information fields, and therefore do not fit within any of the AVP types defined above. Complex AVPs MUST provide the data format, and the expected length of the AVP.

5.1 COMMAND-CODE AVP

The Command-Code AVP MUST be the first AVP following the DIAMETER header. A DIAMETER message MUST have at most one Command-Code AVP, and it is used in order to communicate the command associated with the message.

- **Code** – 256
- **Type** – Integer32

5.2 DESTINATION-NAI AVP

This AVP is used to carry the NAI of the destination.

- **Code** – 269
- **Type** - String

5.3 HOME-AGENT-ADDRESS AVP

This AVP contains the Mobile Nodes's Home Agent Address.

- **Code** – 334
- **Type** – Address

5.4 HOST-NAME AVP

The Host-Name AVP is used to inform a DIAMETER peer of the sender's identity. All DIAMETER messages MUST include the Host-Name AVP, which contains the host name of the originator of the DIAMETER message that MUST follow the NAI naming conventions.

- **Code** – 32
- **Type** – String

5.5 IPM-CARE-OF-ADDRESS AVP

This AVP is used to carry the MN's Care-of-Address.

- **Code** – 362
- **Type** - Address

5.6 IPM-CLIENT-ADDRESS AVP

This AVP is used to carry the MN's IP Address, either Static or Dynamic.

- **Code** – 360
- **Type** - Address

5.7 IPM-CONTEXT-DATA AVP

This AVP carries the Context Data of the User at previous SMM. The complex data could contain AVP format data. The Context-Data could potentially carry the QOS information that MN was receiving at previous SMM.

- **Code** – 373
- **Type** - Data

5.8 IPM-CONTEXT-REQUEST-TYPE AVP

This AVP carries the Context requested by the SMM.

- **Code** – 372
- **Type**- Integer32

These carry the current types of various Context Requests.

- Context-Request (0)
- Context-Request with IP-Forwarding (1)
- Context-Request with IP-Buffering (2)

5.9 IPM-HMM-NAI AVP

This AVP is used to carry the HMM's NAI.

- **Code** – 364
- **Type** - String

5.10 IPM-L2-ADDRESS AVP

This AVP carries the L2-Address of IPM Client connection. The AVP carries both the types of Address and Data.

- **Code** – 374
- **Type** – Data

These are the current types supported.

- 802.3 Address (0)
- 802.11 Address (1)
- IMSI (2)
- MIN (3)

5.11 IPM-PROFILE AVP

This AVP carries the Profile of the User, who is registering. The complex data could contain AVP format data.

- **Code** – 371
- **Type** - Data

5.12 IPM-PROFILE-TYPE AVP

This AVP carries the user Profile requested by SMM with the IRR message.

- **Code** – 370
- **Type** – Integer32

The current Profile types are:

- Partial (0) – Minimal Profile required.
- Full (1) – Complete Profile of the user.

5.13 IPM-REGISTRATION-CANCELLATION-REASON AVP

This AVP carries the reason for the Registration Cancellation Message being sent by MNN to SMM.

- **Code** – 375
- **Type** – Integer32

5.14 IPM-REGISTRATION-REPLY AVP

This AVP carries IPM Registration-Reply Message received from the HMM to SMM.

- **Code** – 367
- **Type** - Data

5.15 IPM-REGISTRATION-REQUEST AVP

This AVP carries either complete or partial IPM-Registration Request received from the MN.

- **Code** – 366
- **Type** - Data

5.16 IPM-REGISTRATION-RESPONSE-CODE AVP

This AVP carries the Registration-Response-Code.

- **Code** – 368
- **Type** – Integer32

5.17 IPM-REGISTRATION-TYPE AVP

This AVP is used to carry the type of Registration.

- **Code** – 361
- **Type** – Integer32

These are the current values supported:

- Initial Registration (0)
- De-Registration (1)
- System-Change (2)
- ANI-Change (3)
- Local Re-Registration (4)

- Re-Registration (5)
- Clean-Up (6)
- Location-Update (7)
- Admin-Initiated-Clean-Up (8)

5.18 IPM-ROUTING-AREA-NAI AVP

This AVP carries the ANI's NAI, where the MN is currently registered.

- **Code** – 365
- **Type** - String

5.19 IPM-SMM-MN-KEY AVP

This AVP carries the shared secret key between SMM and MN. This key is only valid for the session.

- **Code** – 376
- **Type** - Data

5.20 IPM-SMM-NAI AVP

This AVP carries the SMM's NAI.

- **Code** – 363
- **Type** - String

5.21 IPM-TERMINAL-TYPE AVP

This AVP carries the Terminal Type of MN.

- **Code** – 369
- **Type** – Integer32

These are the current Terminal-Types supported.

- 802.3 Type Terminal (1)
- 802.11 Type Terminal (1)
- IS91 Type Terminal (2)
- IS36 Type Terminal (3)
- IS96 Type Terminal (4)
- Modem (5)
- Unknown Terminal (#ffffffff)

5.22 INTEGRITY-CHECK-VALUE AVP

The Integrity-Check-Value AVP is used for hop-by-hop message authentication and integrity.

- **Code** – 259
- **Type** - Complex

5.23 NONCE AVP

The Nonce AVP MUST be present prior to the Integrity-Check-Value AVPs within a message and is ued to ensure randomness within a message.

- **Code** – 261
- **Type** - Data

5.24 PROXY-STATE AVP

The Proxy-State AVP is used by proxy servers when forwarding requests and contains opaque data that is used by the proxy to further process the response.

- **Code** – 33
- **Type** - Address

5.25 RESULT-CODE AVP

The Result-Code AVP indicates whether a particular request was completed successfully or whether an error occurred.

- **Code** – 268
- **Type** - Complex

5.26 TIMESTAMP AVP

The Timestamp AVP is used to add replay protection to the DIAMETER protocol. This AVP MSUT appear prior to the Integrity-Check-Value AVP or any other message integrity AVP defined in separate extensions.

- **Code** – 262
- **Type** – Time

5.27 USER-NAME AVP

The User-Name AVP contains the User-Name in a format consistent with the NAI specification. All DIAMETER systems SHOULD support usernames of at least 72 octets in length.

- **Code** – 1
- **Type** - String

6. ATTRIBUTES

Data Attribute is a payload for extensions. The format of the Data Attributes provides the flexibility for representation of many different types of information. There can be multiple Data Attributes within any extension payload. The length of Data Attributes will either be 2 octets or defined by the payload length field.

Attr Type	AF	Sub-Type	Payload Length
Attribute Value AF = 0 TLV; AF = 1 TV			

- **Attr Type (1 octet)** – Unique identifier for each type of attribute.
- **Sub-Type (1 octet)** – Defines the attribute sub-type.
- **AF Bit** – Attribute format indicates whether the data attribute follows the type Type/Value (TV) format (AF=1) or follows the Type/Length/Value (TLV) format (AF=0).
- **Payload Length (2 octets)** – Length in octets of the attribute value. When the AF bit is 1, the attribute value is 2 octets and payload length field is not present.
- **Attribute Value (Variable Length)** – It is the value of the attribute. If the AF bit is 0, this field has a variable length defined by the payload length field. If the AF is 1, the attribute value has a length of 2 octets.

6.1 ACCOUNT NUMBER DATA ATTRIBUTE

The Account Number Data Attribute defines the User's account number assigned by the ISP.

Attr Type = 1	AF	Sub-Type	Payload Length = 4
Account Number Value			

- AF – 0.
- **Attr Type** – 1.
- **Sub-Type** – The following sub-types are defined for this attribute:
  - 0, The default sub-type, the value is sent in clear.
  - 1, Secret key encryption using the shared secret key between the user and its home domain. This type of encryption provides data confidentiality.
  - 2, Public key encryption using the user's private key. This type of encryption provides data confidentiality and digital signature.
  - 3, Public key encryption using the home domain public key. This type of encryption provides data confidentiality.
- Payload Length – 4.
- Account Number Value – It is the value of the account number.

6.2 DATA AUTHENTICATION REPLY ATTRIBUTE

The Data Authentication Reply Attribute carries the authenticator, which is the result of running the hash function on the authentication data provided in the Data Authentication Request Attribute.

Attr Type =24	AF	Sub-Type	Payload Length
Authenticator Data.....			

- **AF** – 0.
- **Attr Type** – 24.
- **Sub-Type** – The following sub-types are defined for this attribute:
  - 0, The default sub-type, the value is sent in clear.
  - 1, Secret key encryption using the shared secret key between the user and its home domain. This type of encryption provides data confidentiality.
  - 2, Public key encryption using the user's private key. This type of encryption provides data confidentiality and digital signature.
  - 3, Public key encryption using the home domain public key. This type of encryption provides data confidentiality.
- **Payload Length** – Variable.
- **Authenticator Data** – It is the data resulted from running the hash function on the authentication data provided by the Data Authentication Request Attribute.

6.3 DATA AUTHENTICATION REQUEST ATTRIBUTE

The Data Authentication Request Attribute is used to carry the data, which needs to be authenticated by the IPM Security Center by running the hash function on this data.

Attr Type =23	AF	Sub-Type	Payload Length
Authentication Data.....			

- **AF** – 0.
- **Attr Type** – 23.
- **Sub-Type** – The following sub-types are defined for this attribute:
  - 0, The default sub-type, the value is sent in clear.
  - 1, Secret key encryption using the shared secret key between the user and its home domain. This type of encryption provides data confidentiality.
  - 2, Public key encryption using the user's private key. This type of encryption provides data confidentiality and digital signature.

- 3, Public key encryption using the home domain public key. This type of encryption provides data confidentiality.

- **Payload Length** – Variable.
- **Authentication Data** – It is the control message data, which needs to be authenticated by the IPM Security Center by running the hash function on this data.

6.4 DIGITAL SIGNATURE DATA ATTRIBUTE

The Digital Signature Data Attribute defines the User's Digital Signature, which is created by running a hash function H (e.g. MD5) over a message fragment. This Attribute should be encrypted using the full secret key between the MN and its home domain or the private key for the MN.

Attr Type = 11	AF	Sub-Type	Payload Length
Digital Signature Value.....			

- **AF** – 0.
- **Attr Type** – 11.
- **Sub-Type** – The following sub-types are defined for this attribute:

  - 0, The default sub-type, the value is sent in clear.
  - 1, Secret key encryption using the shared secret key between the user and its home domain. This type of encryption provides data confidentiality.
  - 2, Public key encryption using the user's private key. This type of encryption provides data confidentiality and digital signature.
  - 3, Public key encryption using the home domain public key. This type of encryption provides data confidentiality.

- **Payload Length** – Variable.
- **Digital Signature Value** – Is a sequence of bytes generated from running a hash function over all the attribute's payload for the User Authentication Information Extension.

6.5 DUPLICATE SECRET KEY REPLY DATA ATTRIBUTE

The Duplicate Secret Key Reply Data Attribute carries the session key information, which is allocated by IPM Security Center. Another encrypted copy is generated and sent in conjunction with the original one. This attribute can be included in the Session Key Allocation Extension when the extension sub-type field value is 3.

Attr Type = 22		AF	Sub-Type	Payload Length
Rsv	Rn		Key Length	rsv
Liftetime				
Key ID				
SPI				
Key Data.....				
Encrypted Deuplicate Key Data.....				

- **Attr Type** – 22
- **AF** - 0
- **Sub-Type** - The following types are defined:
  - 0, The default sub-type, the value is sent in clear.
  - 1, Secret key encryption using the shared secret key between the user and its home domain. This type of encryption provides only data confidentiality.
  - 2, Public key encryption using the user's private key. This type of encryption provides data confidentiality and digital signature. .
- **Payload Length (2 octets)** - It is 8 + SPI length + key data length.
- **Lifetime** – It is the key lifetime. After a lifetime expires the same key might be reassigned to somebody else.
- **SPI (4 octets)** - It is the Security Parameter Index. This SPI in conjunction with the generated key will be used to define a security association between two entities (e.g. MN and HMM, MN and SMM).
- **Key ID (4 octets)** - It is the key unique identifier issued by the IPM Security Center.
- **Key Data (Variable)** – It is the secret key generated by the IPM Security Center.
- **Encrypted Duplicate Key Data** – A copy from the key data encrypted by the method defined by the sub-type field.

6.6 SSN DATA ATTRIBUTE

The SSN Data Attribute defines the User's SSN.

Attr Type = 2	AF	Sub-Type	Payload Length = 4
		SSN Value	

- **AF** – 0.
- **Attr Type** – 2.
- **Sub-Type** – The following sub-types are defined for this attribute:
  - 0, The default sub-type, the value is sent in clear.

- 1, Secret key encryption using the shared secret key between the user and its home domain. This type of encryption provides data confidentiality.
- 2, Public key encryption using the user's private key. This type of encryption provides data confidentiality and digital signature.
- 3, Public key encryption using the home domain public key. This type of encryption provides data confidentiality.

- **Payload Length** – 4.
- **SSN Value** – The value of the SSN.

6.7 SECRET KEY REQUEST DATA ATTRIBUTE

The Secret Key Request Data Attribute is used to request a dynamically allocated session secret key with a specific length from the IPM Security Center. The Session Key Allocation Request Extension **MAY** have multiple Secret Key Request Data Attributes.

Attr Type = 20	AF	Sub-Type	Key Length	ET	rn

- **Attr Type** – 20
- **AF** - 1
- **Sub-Type** - The following types are defined:

  - 0, A single key will be allocated and encrypted using the Encryption type.
  - 1, A single key is allocated and duplicated. The duplicate will be encrypted by the encryption method defined by the Encryption Type field.

- **Encryption Type (ET)** – The following Encryption Types are defined:

  - 0, The default sub-sype, the value is sent in clear.
  - 1, Secret key encryption using the shared secret key between the user and its home domain. This type of encryption provides only data confidentiality.
  - 2, Public key encryption using the user's private key. This type of encryption provided data confidentiality and digital signature.

- **Key Length** – Length of the key needed to be allocated.
- **rn** – It is a number from 1 to 15 which distinguishes between the different key allocation requests issued to the IPM Security Center. The issuer of the request will use the rn to match the key allocation request with the Key Allocation Reply.

6.8 SINGLE SECRET KEY REPLY DATA ATTRIBUTE

The Single Secret Key Reply Data Attribute carries the session key information, which is allocated by the IPM Security Center. This attribute is carried by the Session Key Allocation Extension when the extension Sub-Type value is 2.

Attr Type = 21		AF	Sub-Type	Payload Length
Rsv	Rn	Key Length		rsv
Liftetime				
Key ID				
SPI				
Key Data.....				

- **Attr Type** – 21
- **AF** - 0
- **Sub-Type** - The following types are defined:
  - 0, The default Sub-Type, the value is sent in clear.
  - 1, Secret key encryption using the shared secret key between the user and its home domain. This type of encryption provides only data confidentiality.
  - 2, Public key encryption using the user's private key. This type of encryption provides data confidentiality and digital signature. .
- **Payload Length (2 octets)** - It is 8 + SPI length + key data length.
- **Lifetime (4octets)** – It is the key lifetime.
- **SPI (4 octets)** - It is the Security Parameter Index. This SPI in conjunction with the generated key will be used to define a security association between two entities (e.g. MN and HMM, MN and SMM).
- **Key ID (4 octets)** - It is the key unique identifier issued by the IPM Security Center.
- **Key Data (Variable)** – It is the secret key generated by the IPM Security Center.

6.9 USER ADDRESS DATA ATTRIBUTE

The User Address Data Attribute defines the User's current address.

Attr Type = 6	AF	Sub-Type	Payload Length
User Address Value.....			

- **AF** – 0.
- **Attr Type** – 6.
- **Sub-Type** – The following sub-types are defined for this attribute:

- 0, The default sub-type, the value is sent in clear.
- 1, Secret key encryption using the shared secret key between the user and its home domain. This type of encryption provides data confidentiality.
- 2, Public key encryption using the user's private key. This type of encryption provides data confidentiality and digital signature.
- 3, Public key encryption using the home domain public key. This type of encryption provides data confidentiality.

- **Payload Length** – Variable.
- **User Address Value** – This field contains a string of the following format:

User Address::= country +(" ") State +(" ") city +(" ")
Street [+(" ") aptn]
country::= "cny" "=" String
state::= "ste" "=" String
city::= "cty" "=" String
street::= "str" "=" String
aptn::= "apt" "=" String

6.10 USER BIRTHDAY DATA ATTRIBUTE

The User Birthday Data Attribute defines the User's birthday.

Attr Type = 4	AF	Sub-Type	Payload Length
User Birthday Value.....			

- **AF** – 0.
- **Attr Type** – 4.
- **Sub-Type** – The following sub-types are defined for this attribute:

  - 0, The default sub-type, the value is sent in clear.
  - 1, Secret key encryption using the shared secret key between the user and its home domain. This type of encryption provides data confidentiality.
  - 2, Public key encryption using the user's private key. This type of encryption provides data confidentiality and digital signature.
  - 3, Public key encryption using the home domain public key. This type of encryption provides data confidentiality.

- **Payload Length** – Variable.
- **User Birthday Value** – This field contains a string of the following format:

User Birthday ::= month +(" ") day + (" ") + year
Month ::= "mth" "=" String
Day ::= "day" "=" String
Year ::= "yer" "=" String

Example: mt=07 day=09 yer=1966

6.11 USER HOME PHONE NUMBER DATA ATTRIBUTE

The User Home Phone Number Data Attribute defines the User's home phone number.

Attr Type = 7	AF	Sub-Type	Payload Length
User Home Phone Number.....			

- **AF** – 0.
- **Attr Type** – 7.
- **Sub-Type** – The following sub-sypes are defined for this attribute:
  - 0, The default sub-type, the value is sent in clear.
  - 1, Secret key encryption using the shared secret key between the user and its home domain. This type of encryption provides data confidentiality.
  - 2, Public key encryption using the user's private key. This type of encryption provides data confidentiality and digital signature.
  - 3, Public key encryption using the home domain public key. This type of encryption provides data confidentiality.
- **Payload Length** – Variable.
- **User Home Phone Number** – This field contains a string representing the user phone number.

Example: 972-685-1234

6.12 USER NAI DATA ATTRIBUTE

The User NAI Data Attribute defines the User Network Access Identifier.

Attr Type = 9	AF	Sub-Type	Payload Length
NAI.....			

- **AF** – 0.
- **Attr Type** – 9.
- **Sub-Type** – The following sub-types are defined for this attribute:
  - 0, The default sub-type, the value is sent in clear.

- 1, Secret key encryption using the shared secret key between the user and its home domain. This type of encryption provides data confidentiality.
- 2, Public key encryption using the user's private key. This type of encryption provides data confidentiality and digital signature.
- 3, Public key encryption using the home domain public key. This type of encryption provides data confidentiality.

- **Payload Length** – Variable.
- **User NAI** – This field contains a string representing the User Network Access Identifier.

Example: mkhalil@nortelnetworks.com

6.13 USER NAME DATA ATTRIBUTE

The User Name Data Attribute defines the User's full name.

Attr Type = 3	AF	Sub-Type	Payload Length
User Name Value			

- **AF** – 0.
- **Attr Type** – 3.
- **Sub-Type** – The following sub-types are defined for this attribute:

  - 0, The default sub-type, the value is sent in clear.
  - 1, Secret key encryption using the full secret key between the user and its home domain. This type of encryption provides data confidentiality
  - 2, Public key encryption using the user's private key. This type of encryption provides data confidentiality and digital signature.
  - 3, Public key encryption using the home domain public key. This type of encryption provides data confidentiality.

- **Payload Length** – Variable.
- **User Name Value** – This field contains a string of the following format:

  User_Name ::= last_name +(" ") first_name +(" ") mid_name
  Last_name ::= LAST_NAME "=" String
  First_name ::= FIRST_NAME "=" String
  mid_name ::= MID_NAME "=" String
  LAST_NAME ::= "ln"
  FIRST_NAME ::= "fn"
  mid_name ::= "mn"

6.14 USER PASSWORD DATA ATTRIBUTE

The User Password Data Attribute defines the User's password.

Attr Type = 5	AF	Sub-Type	Payload Length
Password Value.....			

- **AF** – 0.
- **Attr Type** – 5.
- **Sub-Type** – The following sub-types are defined for this attribute:
  - 0, The default sub-type, the value is sent in clear.
  - 1, Secret key encryption using the shared secret key between the user and its home domain. This type of encryption provides data confidentiality.
  - 2, Public key encryption using the user's private key. This type of encryption provides data confidentiality and digital signature.
  - 3, Public key encryption using the home domain public key. This type of encryption provides data confidentiality.
- **Payload Length** – Variable.
- **Password Value** – The string which represents the User's password.

6.15 USER PIN NUMBER DATA ATTRIBUTE

It is an integer value selected by the user to secure access to his account This Attribute **MAY** be included with User Authentication Information Extension.

Attr Type =10	AF	Sub-Type	Payload Length
User PIN Number.....			

- **AF** – 0.
- **Attr Type** – 10.
- **Sub-Type** – The following sub-types are defined for this attribute:
  - 0, The default sub-type, the value is sent in clear.
  - 1, Secret key encryption using the shared secret key between the user and its home domain. This type of encryption provides data confidentiality.
  - 2, Public key encryption using the user's private key. This type of encryption provides data confidentiality and digital signature.
  - 3, Public key encryption using the home domain public key. This type of encryption provides data confidentiality.
- **Payload Length** – 4 octets.

- **User PIN Number** – This field contains a string representing the User PIN number.

Example: 1234abcd567

6.16 USER WORK PHONE NUMBER DATA ATTRIBUTE

The User Work Phone Number Data Attribute defines the User's work phone number. One or more of these Attributes may be included with the User Authentication Information Extension.

Attr Type = 8	AF	Sub-Type	Payload Length
User Work Phone Number.....			

- **AF** – 0.
- **Attr Type** – 8.
- **Sub-Type** – The following sub-types are defined for this attribute:
  - 0, The default sub-type, the value is sent in clear.
  - 1, Secret key encryption using the shared secret key between the user and its home domain. This type of encryption provides data confidentiality.
  - 2, Public key encryption using the user's private key. This type of encryption provides data confidentiality and digital signature.
  - 3, Public key encryption using the home domain public key. This type of encryption provides data confidentiality.
- **Payload Length** – Variable.
- **User Work Phone Number** – This field contains a string representing the User work phone number.

Example: 972-685-1234

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLATED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER :** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents *will not* correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.